第38卷 第24期 计 算 机 工 程 2012年12月
Vol.38 No.24 Computer Engineering December 2012

·云计算专题· 文章编号：1000—3428(2012)24—0001—04 文献标识码：A 中图分类号：TP309

基于整数多项式环的全同态加密算法

徐 鹏，刘 超，斯雪明

(信息工程大学信息工程学院，郑州 450002)

摘 要：为确保云计算环境下用户数据的安全性，利用同态加密算法对数据和加密函数的隐私保护功能，设计一种基于整数多项式环的全同态加密算法。该算法包括同态算法和重加密算法，前者针对明文数据进行加密，后者针对密文数据进行二次加密。分析结果表明，该算法的计算复杂度为 $O(n^5)$，低于理想格全同态加密算法。

关键词：全同态加密算法；云计算安全；数据加密；理想格；近似最大公约数；隐私保护

Fully Homomorphic Encryption Algorithm Based on Integer Polynomial Ring

XU Peng, LIU Chao, SI Xue-ming

(School of Information Engineering, Information Engineering University, Zhengzhou 450002, China)

【Abstract】To ensure the user data security under cloud computing environment, this paper uses homomorphism encryption algorithm for data and encryption function of privacy protection function, and designs a new fully homomorphic encryption algorithm based on integral polynomial ring. Both the homomorphic encryption and the re-encryption are included in the algorithm. The homomorphic encryption is used to encrypt the data, and re-encryption is used to encrypt the encrypted data. Analysis result shows that the proposed algorithm computing complexity $O(n^5)$ is lower than ideal lattice fully homomorphic encryption.

【Key words】fully homomorphic encryption algorithm; cloud computing security; data encryption; ideal lattice; approximate Greatest Common Divisor(GCD); privacy protection

DOI: 10.3969/j.issn.1000-3428.2012.24.001

1 概述

2008 年底，IBM 公司向全球推出了“智慧地球”这个愿景，其目标是让世界的运转更加智能化，让个人、企业、组织、政府、自然和社会之间的互动效率更高。云计算作为一种新兴的计算模式，是帮助实现“智慧地球”的最重要的手段之一。2007 年，在百度中搜索“云计算”，智能找到不超过 40 个搜索结果，但是 4 年后的今天，这个数字已经超过 3 860 万。市场分析师和权威媒体已经预测：在未来的 5 年内，绝大多数公司将采纳云计算。目前，认识并应用云计算已经成为企业和政府把握市场脉搏的必修课。但是云计算的发展存在巨大的瓶颈，那就是云计算的安全问题。IDC 在去年公布的一份调查报告中指出，在 244 个 IT 主管/CIO 中，75%的受访者认为对于云计算，安全性是重要或非常重要挑战。云计算在某种程度上模糊了静止数据、传输中的数据以及使用中的数据之间的区别，这使得数据加密成为最重要的防御手段之一。因此，建立一个数据加密策略并且实现某种技术对它进行支持是最好的主动防御措施。

云计算不断发展，改变了现有数据加密的方式。用户的数据可以分为 2 类：存储数据，即不需要加密的数据；隐私数据，即需要加密的数据。在云环境下，用户对存储介质提出了担忧：服务器端保密机制不完善，信誉无法保证，安全隐患不能完全解决。如何把私有的信息传递到网络服务器端是云计算安全问题的一个研究热点。数据隐私研究公司波耐蒙研究所的 Ponemon L 表示：“确保数据在网上的安全性，一个肯定管用的办法就是使用加密技术。把文件保存到网络上之前先进行加密，这意味着除了用户，谁也无法获取文件里面的敏感信息——不管这个文件最终出现在哪里。”加密技术固然是一个非常理想的方法，但是服务器端对加密信息进行处理后用户并不能确定私有的加密数据可以恢复。文献[1]提出隐私加密，主要解决的问题是数据库中针对密文数据修改以后并能恢复明文的加密算法。但是由于隐私加密技术在改进和实现过程中并不能很好地克服密文数据扩张和复杂度的降低，因此并

基金项目：国家“863”计划基金资助项目“新概念高效能计算机体系结构及系统研究开发”(2009AA012201)

作者简介：徐 鹏(1986－)，男，硕士，主研方向：云计算，信息安全；刘 超，讲师；斯雪明，副研究员

收稿日期：2012-06-08 **修回日期：**2012-06-30 **E-mail：**royalfei1124@gmail.com

没有得到很好的发展[2-6]。现有的密码算法都是数据加密的可选算法。在云背景下，服务器端需要对用户加密后的数据进行操作，但是现有的密码算法都遵循雪崩效应，针对密文的任何操作都是无法恢复明文。因此，在新形势下，加密过后的密数据应该可以进行操作(例如模运算、求和、求均值等)，但仍然可以恢复明文。以解决密文数据 2 次加密问题的同态加密算法是满足用户和商家需要的理想加密算法。1990 年至 2011 年间，随着研究人员和研究机构的关注同态加密算法得到了发展。

文献[7]实现了理想格全同态加密算法。全同态加密算法设计的目的是可对密文数据进行操作，并且仍可恢复明文数据。该方案主要依赖于多项式环中理想格的基的矩阵和向量运算(向量的加法和乘法)，每一个循环都要分别计算每个元素(元素就是向量)，计算完矩阵后还要处理明文本身，整个算法的复杂性高，只能加密单个比特，使得矩阵和向量的加密方法实用性不强。文献[8]提出一种全新的基于整数的全同态加密体制，把原始的理想格方法改进为只利用加法、乘法和模运算代替基于多项式环的理想格，这样能提高计算效率，降低复杂度。全同态加密算法是近年来解决云计算安全问题中数据加密的研究热点[9-13]。

到目前为止，全同态加密算法已经在匿名投票、垃圾邮件过滤等诸多实用领域得到一定的应用。在云模式下，如何能够更好地控制子系统，实现信息的保密传递等方面还没有得到广泛的探讨。因此，针对这些问题，本文主要完成以下两方面的研究工作：(1)对于全同态加密算法区别于其他算法信息保密和函数保密的分析。(2)设计一种复杂度低于理想格全同态加密算法。

2 基于整数环的全同态加密算法

2.1 全同态加密算法发展现状及数据保护特点

全同态加密算法颠覆了传统意义下的加密模式(图 1、图 2)，它是一种可以对密文进行操作但仍可以恢复明文的加密算法。算法设计的目的是：解决云环境下数据上传服务器端，Sever 不可信，用户把私有数据加密上传服务器端。全同态加密算法最终实现：

$$Decrypt'(sk, Evaluate(pk, C, c)) = C(m_1, m_2, \cdots, m_t)$$

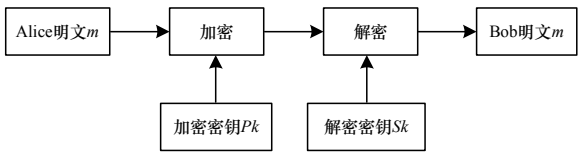

图 1 原始信息加解密示意图

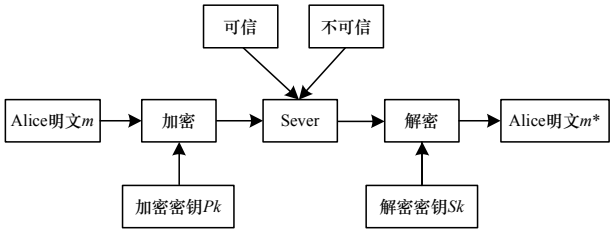

图 2 云背景下信息加解密示意图

这样用户可以把私有信息经过加密上传服务器端，享受云服务，但是服务器端并不能获得用户数据。因此全同态加密算法可针对用户的需求满足对加密信息和加密函数的保护，使得在整个传递过程当中始终保持加密状态。

加密信息的处理如图 3 所示，主要是对私有信息进行保护。Alice 有私有的函数 f_A 和私有的信息 x_A，Bob 把私有信息 y_B 用私有公钥 pk_B 加密得到 $E(y)$ 发送给 Alice，Alice 用自己的私有函数 f_A 加密私有信息 x_A 和 $E(y_B)$，由于同态性质，函数 f_A 被隐藏，而 Bob 获得 $E(f_A(x_A, y_B))$。Bob 通过私有的私钥加密 $D(E(f_A(x_A, y_B))) = f_A(x_A, y_B)$。

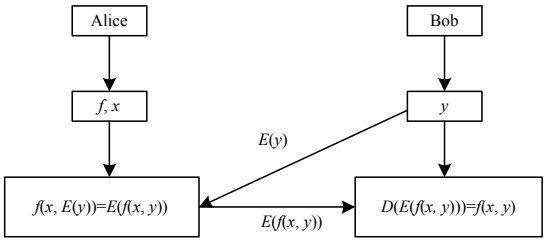

图 3 加密信息处理

加密函数的处理如图 4 所示，主要是对私有的操作函数进行保护。Alice 有私有的函数 f_A，并用私有公钥 pk_A 加密函数 f_A 发送给 Bob，Bob 根据私有信息 x_B 计算 $E(f_A)(x_B)$，由于同态性质，因此隐藏了 Bob 的信息 x_B，得到 $E(f_A(x_B))$，并发送给 Alice，Alice 用私钥解密获得 $f_A(x_B)$。

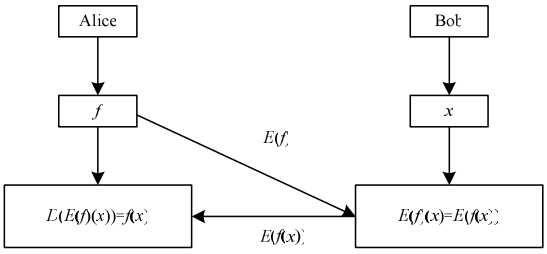

图 4 加密函数处理

2.2 整数环全同态加密算法分析

由于理想格全同态加密算法复杂度高，且密文数据扩张不能得到解决，因此实用性不强。根据已有的理想格和整数全同态加密算法，设计基于 $F_p[x]$ 的全同态加密算法。

同态算法具体如下：

KeyGen：对 $f(x) \in F_p[x]$，选择随机的整数 $a_i, r_i \in Z$，因此公钥 $pk = < b_0, b_1, \cdots, b_n >$，对每个 b_i，满足 $b_i = a_i f(x) + r_i$，b_0 最大。

Encryption：随机选择一个整数子集 $S \in \{1, 2, \cdots, n\}$，$m \in \{0, 1\}$，随机选择 $r \in (-2^{2\rho}, 2^{2\rho})$，密文 $c_i = [m + 2r + 2\sum_{i \in S} b_i] \bmod b_0$。

Decryption：$m = [c \bmod x] \bmod 2$。

同态性性质：

(1)加法：给定公钥 pk，密文 c_1、c_2，则：

$c = [c_1 + c_2] \bmod b_0$

(2)乘法：给定公钥 pk，密文 c_1、c_2，则：

$c=[c_1\cdot c_2]\bmod b_0$

其中，$\lfloor x\rfloor$表示x向下取整；$\lceil x\rceil$表示x向上取整。

加解密正确性分析：

(1)设需要加密的明文信息为$m=1$或$m=0$，选择的函数为$f_i(x)$，选择$n+1$个a_i和$n+1$个r_i，$S=\{1,2,\cdots,n\}$。

(2)计算$n+1$个b_i，使得b_0次数最高。

(3)加密明文信息m，得到$c=[m+2r+2\sum_{i\in S}b_i]\bmod b_0$。

(4)不妨设i取得S集合中的前k个b_i。

(5)密文c可以写成：

$c=\left[m+2r+2(b_1+b_2+\cdots+b_k)\right]\bmod b_0$

(6)c是满足多项式形式的数据，即$c=g(x)x+r'$。

(7)解密时，首先$c\bmod x$得到h，其中，$h=r'=m+2(r+r_1+r_2+\cdots+r_k)$。

(8)最后$h\bmod 2$得到密文m。

同态算法正确性分析：

(1)设$C=\{c_1,c_2,\cdots,c_n\}$，$c=[m+2r+2\sum_{i\in S}b_i]\bmod b_0$。

(2)$H(pk,C)=(c_1*c_2*\cdots*c_n)\bmod b_0$，其中，$*$表示同态加法或者同态乘法。

(3)$D(sk,H(pk,C))=$

$\left(\left((c_1*c_2*\cdots*c_n)\bmod b_0\right)\bmod x\right)\bmod 2$。

(4)恢复得到明文$m=(m_1*m_2*\cdots*m_n)$。

定义1 给定一个随机选择的整数集$S=\{x_0,x_1,\cdots,x_n\}$，每一个x_i都是接近于大素数p，p是这些整数的近似公因子，寻找这个近似公因子p的问题称为近似最大公约数(Greatest Common Divisor, GCD)问题。

定义2 给定一个整数集合$S=\{a_1,a_2,\cdots,a_n\}$和一个整数x，是否存在一个非空子集$H\in S$，满足H中所有元素之和等于x，该问题称为离散子集求和问题(Sparse Subset Sum Problem, SSSP))[14-16]。

定理 基于整数环$F_p[x]$全同态加密算法中同态加密算法安全性依赖于离散子集求和问题。

证明：由于同态算法中公钥为$pk=<b_1,b_2,\cdots,b_n>$，对于每一个$b_i=a_if_i(x)+r_i$，因此通过每一个$f_i(x)$可以得到一组约化基$A=<g_1,g_2,\cdots,g_t>$，$t\leqslant n$，每一个b_i都可以通过约化基A表示得到，令约化基$A=<g_1,g_2,\cdots,g_t>$为一个集合，给定b_i，找出满足$b_i=a_i\left(\sum_{j\in\{1,2,\cdots,t\}}h_ig_i\right)+r_i$的$g_i$，$h_i\in Z$，满足SSSP的定义。证毕。

针对离散子集求和问题的攻击都是在限定的参数范围内实现的(例如，集合个数的选择、因子的大小等)，而且攻击算法复杂度高，在文献[15]中有一个折中攻击算法，其复杂度约为$\gamma_{\text{set}}(n)^{O(\gamma_{\text{subset}}(n))}$。文献[16]给出一个针对SSSP问题的基于格的密码分析算法，需要的时间复杂度仍然是指数级。

根据文献[7]对随机数选择可以得出：通过密文c重加密得到的新密文数据c_{new}，选择的随机参数r满足$|2r|<(p/8)^{1/2}$，这样选择得到的密文更安全。

重加密算法Evaluate具体如下：

Keygen：按照上述算法选择公钥pk和私钥sk，选择k，其中，k是满足计算安全的大素数；p是同态算法中的$F_p[x]$，定义$x_p=\left\lfloor 2^k/p-1/2\right\rfloor$，汉明重量为$\theta$的多项式$g(x)=\sum g_ix^i$，$\theta$为2个$a_i$的最大距离，$c_i\in Z\cap[0,2^{k+1})$，使得$\sum_{i\in S}c_i=x_p\left(\bmod 2^{k+1}\right)$，$y_i=c_i/2^k$，因此可以得出$\sum_i y_i=1/p\bmod 2$，得到新公钥$pk^*=<pk,y_1,y_2,\cdots,y_n>$，新私钥$sk^*=<g_1,g_2,\cdots,g_n>$。

Encryption：

输入：密文c，新公钥pk^*；

输出：新密文$c^*=[c\cdot y_i]\bmod 2$。

Decryption：

输入：新密文c^*；

输出：密文$c=\left[c^*-\left\lceil\sum_{i\in S}c_ig_i-1/2\right\rceil\right]\bmod 2$。

整个算法的设计思路是通过多项式的次数、模运算、交互运算以达到混乱明文的作用。在设计过程中主要是考虑把问题的复杂性归结到离散子集求和问题，因此，选择多项式是该算法的关键环节，多项式的选择可以根据加密方对安全的要求程度决定，例如安全程度低可以选择$f(x)=x+1$，如果安全程度高可以通过提升$f(x)$的次数来加强。同态算法的设计还是延续了理想格方法和整数方法的特点，使得循环操作环节简单，便于实际应用。

性质 基于整数环$F_p[x]$的全同态加密算法计算量是$O(n^5)$。

证明：在Evaluate运算中，需要确定x_p、c_i、y_i、Encryption和Decryption 5个部分，输入的$pk=\{b_1,b_2,\cdots,b_n\}$有$n$个，需要计算量为$n$；$c_i=[m+2r+\sum_{i\in S}b_i]\bmod b_0$，计算量为$n$；加密运算和解密运算需要计算量为$n$；每个重加密运算都需要$n$次操作，所以，计算量大约为：

$O(n*n*n*n*n=n^5)$

在实际应用中，存在匿名同态协议和一种半匿名，即相邻结点间不是匿名的，非相邻结点间是匿名的。另外还存在一个乐观可信第三方(optimistic trusted third party)，用于解决当出现非法访问时去找到那个非法访问者，该TTP只有在出现问题时才存在，所以不会影响效率。同态加密技术的快速发展，在云数据检索、投票、垃圾邮件过滤、信号分析领域都有着广泛的应用。在安全协议上，同态算法都是解决一些关键问题的有效方法和手段。

3 算法性能比较

全同态加密算法的主要优势是可以针对密文进行操作，仍然可以回复明文，因此，满足用户对云服务的基本要求。本文算法与2种全同态加密算法进行比较(表1)：

(1)理想格全同态加密算法：需要进行矩阵运算和向量模运算(向量的加法和乘法)，每加密一个比特都需要进行矩阵和向量运算(表示为连续性不好)，公钥扩展$O(n^7)$，每

个 Evaluate 中计算门的计算量为 $O(n^6)$。

(2)整数全同态加密算法：需要进行整数模运算，连续性好， Evaluate 算法中输入超过本身算法要求，就不会实现全同态的性质，存在攻击危险。每个 Evaluate 中计算门的计算量为 $O(n^3)$。

(3)整数环全同态加密算法：主要进行多项式运算，加密过程中不需要重新选择多项式(连续性好)，Evaluate 中计算门的计算量为 $O(n^5)$，根据实际安全的级别进行筛选。

表 1 3 种全同态加密算法性能比较

算法	连续性	计算量	安全性问题	公钥选择	其他性质
理想格全同态加密算法	不好	$O(n^6)$	离散子集求和问题	矩阵	在 Evaluate 操作中随着计算的深入满足全同态
整数全同态加密算法	好	$O(n^3)$	近似 GCD 问题	大整数序列	在 Evaluate 操作中随着计算的深入不满足全同态
整数环全同态加密算法	好	$O(n^5)$	离散子集求和问题	多项式	在 Evaluate 操作中随着计算的深入满足全同态

在算法的设计环节，虽然没有保证严格雪崩效应，但是把算法的安全性依靠在离散子集求和这个难解问题，因此安全性没有受到影响，而且有更好的实现价值。今后需要对降低基于整数多项式环的全同态加密算法的时空开支以及明密文数据的扩散问题进行研究。

4 结束语

全同态加密算法的主要优势是可以针对密文进行操作，仍然可以恢复明文，因此满足用户对云服务的基本要求。本文设计的新算法比原始基于理想格算法复杂度低，在算法的设计环节，虽然没有保证严格雪崩效应，但是将算法的安全性依靠在离散子集求和这个难解问题，因此，安全性没有受到影响，而且有更好的实现价值。下一步工作将降低算法复杂度，并提高加密过程中明文数据的连续性。

参考文献

[1] Rivest R, Adleman L, Dertouzos M. On Data Banks and Privacy Homomorphisms[M]. [S. l.]: Academic Press, 1978: 169-177.

[2] Lipton B. Searching for Elements in Black Box Fields and Applications[C]//Proc. of Cryptology-Crypto'96. [S. l.]: Springer-Verlag, 1996: 283-297.

[3] Domingo-Ferrer J. A Provably Secure Additive and Multiplicative Privacy Homomorphism[C]//Proc. of the 5th International Conference on Information Security. [S. l.]: Springer-Verlag, 2002: 471-483.

[4] Brickell E F, Yacobi Y. On Privacy Homomorphisms[C]//Proc. of Cryptology-EuroCrypt'87. Berlin, Germany: Springer-Verlag, 1987: 117-126.

[5] Feigenbaum J, Merritt M. Open Question, Talk Abstracts, and Summary of Discussions[EB/OL]. (1991-12-05). http://biblioteca.universia.net/html_bura/ficha/params/title/open-questions-talk-abstracts-and-summary-of-discussions/id/46640945.html.

[6] Fellows M, Koblitz N. Combinatorial Cryptosystems Galore![Z]. 1993.

[7] Gentry C. Fully Homomorphic Encryption Using Ideal Lattice[C]//Proc. of STOC'09. [S. l.]: IEEE Press, 2009: 169-178.

[8] van Dijk M, Gentry C, Halevi S, et al. Fully Homomorphic Encryption over the Integers[C]//Proc. of Cryptology-CRYPTO'11. [S. l.]: Springer-Verlag, 2011: 24-43.

[9] Gentry C, Halevi S. Fully Homomorphic Encryption Without Squashing Using Depth-3 Arithmetic Circuits[C]//Proc. of FOCSIEEE'11. [S. l.]: Springer-Verlag, 2011.

[10] Melchor C A, Castagnos G, Gaborit P. Lattice-based Homomorphic Encryption of Vector Spaces[C]//Proc. of ISIT'08. [S. l.]: IEEE Press, 2008: 1858-1862.

[11] Coron J S, Mandal A, Naccache D, et al. Fully Homomorphic Encryption over the Integers with Shorter Public-keys[C]//Proc. of the 31st Annual Conference on Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011.

[12] Chen Y, Nguyen P Q. Faster Algorithms for Approximate Common Divisors: Breaking Fully-homomorphic-encryption Challenges over the Integers[C]//Proc. of Cryptology-EUROCRYPT'12. [S. l.]: Springer-Verlag, 2012.

[13] Chung K M, Kalai Y T, Vadhan S. Improved Delegation of Computation Using Fully Homomorphic Encryption[C]//Proc. of the 30th Annual Conference on Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2010.

[14] Silvano M, Paolo T. Knapsack Problems: Algorithms and Computer Interpretations[M]. [S. l.]: Wiley-Interscience, 1990.

[15] Pfitzmann B, Waidner M. Attacks on Protocols for Server-aided RSA Computation[C]//Proc. of EUROCRYPT'92. Berlin, Germany: Springer-Verlag, 1992.

[16] Nguyen P Q, Shparlinski I. On the Insecurity of a Server-aided RSA Protocol[C]//Proc. of ASIACRYPT'01. London, UK: Springer-Verlag, 2001: 21-35.

编辑 陆燕菲