同态加密研究进展综述*

李 浪[1,2]，余孝忠[1]，杨娅琼[1]，郑兰兰[1]
(1. 衡阳师范学院 计算机科学系，湖南 衡阳 421002；2. 湖南大学 信息科学与工程学院，长沙 410082)

摘 要： 针对云计算中的同态加密问题，进行了相关研究进展综述。介绍了同态密码目前的研究进展，综述了五种典型的公钥同态加密方案和两种典型的全同态加密方案，分析了全同态加密算法的设计方法，并从安全性方面对同态密码学进行了详细的分析和对比，总结对比了四种全同态加密方案，指出全同态密码核心关键问题和进一步需要研究的内容，为同态密码研究提供一定的参考。

关键词： 云计算；信息安全；同态加密
中图分类号： TP309.7 **文献标志码：** A **文章编号：** 1001-3695(2015)11-3209-06
doi:10.3969/j.issn.1001-3695.2015.11.002

Survey on homomorphic encryption technology

Li Lang[1,2], Yu Xiaozhong[1], Yang Yaqiong[1], Zheng Lanlan[1]
(1. *Dept. of Computer Science, Hengyang Normal University, Hengyang Hunan* 421002, *China*; 2. *College of Information Science & Engineering, Hunan University, Changsha* 410082, *China*)

Abstract: This paper reviewed the development of homomorphic encryption. It summarized five typical public key homomorphic encryption scheme and two kinds of typical fully homomorphic encryption scheme, and analyzed the design method of fully homomorphic encryption algorithm. It also analyzed deeply for fully homomorphic encryption from security. This paper compared the four kinds of fully homomorphic encryption algorithm. It pointed out the key problems of fully homomorphic encryption that needed to be researched at present. It can provide reference for further study of homomorphic encryption.

Key words: cloud computing; information security; homomorphic encryption

随着云计算的广泛应用，特别是云平台上的大量电子商务交易，如何安全有效地保护用户隐私与安全成为当今密码学研究领域的热点。若数据以明文形式进行存储则有可能将敏感数据暴露给云服务商，会给用户机密数据带来一系列的安全问题。为解决这一问题，同态加密方案应运而生，利用全同态加密方案对用户数据进行加密，再将密文发送到云端，数据在云端可以进行一系列的上传、下载、删除、更新、检索等操作，且操作的均是密文。该操作既避免了数据在传输过程中被拦截、复制、窜改或伪造等风险，也避免了数据存储方将数据泄露或在服务器端被攻破的危险。

同态加密的研究可以追溯到 20 世纪 70 年代，在 RSA 密码体制刚提出不久，Rivest 等人[1] 提出了全同态加密的概念，也称为隐私同态。这一概念的提出成为密码学界的开放难题，同态加密是一种加密形式，允许用户直接对密文进行特定的代数运算，得到数据仍是加密的结果，与对明文进行同样的操作再将结果加密一样。同态加密优势在于用户在数据加密的情形下仍能对特定的加密数据进行分析和检索，提高了数据处理的效率，保证了数据安全传送，而且正确的加密数据仍能得到正确的解密结果。国外学者相继研究了满足乘法或满足加法的同态加密算法[2~12]，在此基础上还提出了能同时满足有限次乘法与加法的同态密码[13~17]。但直到 2009 年 IBM 研究员 Gentry 才构造出第一个全同态加密方案[18]，解决了困扰密码学界三十多年的难题，同时掀起一股研究全同态加密方案的热潮。全同态加密被认为是解决云计算安全的最好方法，然而目前的全同态加密方案无论是从工程上还是理论研究上都有很多亟待解决的问题。

1 同态加密

1.1 研究进展

同态加密的概念是 1978 年 Rivest 等人在题为《On data banks and privacy homomorphic》中首次提出的，允许用户直接对密文进行特定的代数运算，得到数据仍是加密的结果，与对明文进行同样的操作再将结果加密一样。

公钥密码体制于 1976 年由 Diffie 等人[19] 提出，利用不同密钥将加解密分开实施，为同态加密研究奠定了基础，随后众多优秀的同态加密方案不断涌现。1978 年，Rivest 等人利用数论构造出著名的公钥密码算法 RSA，该算法安全性取决于大整数分解的困难性，具有乘法同态性，但不具备加法同态性。针对此缺陷，Rivest 等人又提出一种同时满足加法同态和乘法同态的 Rivest 方案，其安全性也是取决于大整数的难分解性，实验结果表明，该方案存在严重的安全问题。后有学者提出效果

收稿日期：2015-02-01；修回日期：2015-03-28 基金项目：国家自然科学基金资助项目(61572174)；湖南省自然科学基金资助项目(2015JJ4011)；衡阳师范学院产学研基金资助项目(12CXYZ01)；衡阳师范学院大学生研究性学习和创新性实验计划项目(CX1531)；湖南省重点实验室开放基金资助项目(J1401Z)；湖南省教育厅资助科研重点项目(15A029)

作者简介：李浪(1971-)，男，教授，硕导，博士，主要研究方向为嵌入式系统、信息安全(lilang911@126.com)；余孝忠(1996-)，女，主要研究方向为信息安全；杨娅琼(1994-)，女，主要研究方向为信息安全；郑兰兰(1996-)，女，主要研究方向为信息安全.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

更佳的 MRS 算法。第一个基于离散对数困难的公钥加密体制 ElGamal 于 1984 年提出，该体制具有乘法同态性质[5]；一种满足加法同态的加密方案 GM 算法被 Goldwasse 和 Micali 提出，其安全性是基于二次剩余难题；一种改进的概率同态加密体制于 1994 年被 Benaloh[20] 提出，目前该方案已应用于实际中。1998 年，Okamoto、Naccache 等人分别提出基于加法同态的 OU 和 NS 体制[7,8]，两种体制均能实现多次加法同态运算。第一个基于判定合数剩余类问题的加法同态加密密码体制于 1999 年提出[9]，该体制同样支持多次加法同态运算。2001 年，Damgard 等人[10] 对 Paillier 体制进行了推广，提出了 DJ 体制。在 2005 年第一种同时支持任意多次加法同态和一次乘法同态的 BGN 体制被 Boneh 等人[14] 提出，该方案是距离全同态加密方案最近的一项工作。同年，国内学者在同态密码学研究上也发表了部分成果，我国学者向广利等人[21] 提出了实数范围上的同态加密机制，但并没有得到实际应用。国内学者在探索过程中，也将同态加密技术应用于云计算、多方计算、匿名访问、电子商务等领域，并取得了广泛的成就。2008 年，肖倩等人[22] 提出安全两方的排序方案并将该方案直接扩展到多方排序中；2009 年，邱梅等人[23] 又利用 RSA 密码体制的乘法同态特性，提出了安全多方数据排序方案；2010 年，黄福人[24] 利用 ElGamal 加密体制，提出了拥有匿名性、无数据性、可验证性的电子计票方案；2011 年，张鹏等人[25] 构造了一个可证签名方案，该方案具有可验证性和匿名性等特点，消除了电子计票方案中匿名性与可验证性之间的矛盾；2012 年，李美云等人[26] 在加同态和乘同态的基础上，设计了一种解决云安全存储与信息管理方案，该方案能有效地实现对密文的直接检索、存储，保证了云端用户隐私的安全。同年，Li 等人[27] 对比 DGHV 和 CAFED 方案，提出了一种改进的同态加密算法，同时利用该算法实现了对云存储环境下数据上传、下载、更新、删除、检索等功能。2013 年彭长根等人[28] 在基于大整数分解、离散对数和双线性对等数学问题基础上提出了一个基于同态加密体制的通用可传递签名方案，该方案支持密文运算的特性，实现了可传递签名及验证的一般模型。2014 年杨玉龙等人[29] 提出了一种防止 SQL 注入攻击的同态加密方案，实现了在重要信息保密的情况下获得需求信息。

在同态加密概念提出的三十多年时间里，各种加密方案不断被提出，但这些方案大多是基于半同态加密，几种少数的全同态加密方案由于安全性问题而未能得到实际应用。在半同态加密方案逐渐成熟后，许多学者开始着手全同态加密方案的研究。

1.2 同态加密体制安全分析

安全性是密码算法设计中的首要问题。密码系统中的安全理论基础是计算复杂性理论，用来判断解决一个问题的难易程度。公钥密码体制的安全构造与设计通常基于以下一些计算困难问题。

1) 整数分解问题(integer factorization problem，IFP)

整数分解问题是指任意一个正整数 n，计算其因子表达式 $n=p_1^{e_1},p_2^{e_2},\cdots,p_k^{e_k}$，其中任意 p_i 与 p_j 为两两不同素数，正整数 $e^i\leqslant 1$。

2) 离散对数问题(discrete logarithm problem，DLP)

离散对数问题是指给定素数 p、Z_P^* 的一个生成元 α 以及元素 $\beta\in Z_P^*$，计算整数 x，其中 $0<x\leqslant p-2$，满足成立。

3) 判定合数剩余问题(decisional composite residuosity problem，DCRP)

判定合数剩余问题是指令 $N=pq$，p 和 q 均为大素数，任意给定 $y\in Z_{N^2}^*$，使得 $z=y^N \bmod N^2$，判定 z 为 N 次剩余还是非 N 次剩余。

4) 近似最大公因子问题(approximate GCD problem，AGCDP)

近似最大公因子问题是指给定随机选择的一组整数 x_1，$x_2,\cdots,x_n$，每一个整数 x_i 都接近它们的近似公因子 p，其中 p 是大素数，确定近似公共因子 p 是困难的。

5) 稀疏子集求和问题(spare subset sum problem，SSSP)

稀疏子集求和问题是指给定 m 个 n 比特整数 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 以及一个整数 β，判定是否存在某个子集 $T\subseteq[m]$，使得 $\sum_{i\in T}\alpha_i=\beta$ 成立。

6) 二次剩余问题(quadratic residuosity problem，QRP)

二次剩余问题是指给定一奇合数 n 以及整数 a，两者的雅可比符号为 $\left(\frac{a}{n}\right)=1$，判定 a 是否为一个模 n 的二次剩余数。

1.3 经典同态加密方案

1.3.1 RSA 体制

RSA 密码体制是第一个实用的公钥加密方案，于 1978 年由 Rivest 等人[3] 提出，其安全性是基于整数分解问题的困难性，目前攻击 RSA 的方法有多种，包括大整数分解、欧拉函数值的猜测、迭代攻击、选择明文攻击、定时攻击等。RSA 算法分为以下几个方面描述：

a) 密钥的生成。p 和 q 是满足需要的大素数，$n=pq$，由欧拉定理有 $\varphi(n)=(p-1)\times(q-1)$，其中 $\varphi(n)$ 是 n 的欧拉函数值。随机选择整数 e，满足 $1<e<\varphi(n)$，且 $\gcd(\varphi(n),e)=1$，由 $d\times e\equiv 1 \bmod(\varphi(n))$ 可计算出 d，则公钥 $pk=(n,e)$，私钥 $sk=d$。

b) 加密过程。对于明文空间 M 上的任意明文 m，加密得到密文 $c=E_{pk}(m)=m^e \bmod n$。

c) 解密过程。对于任意密文 c，解密得到明文 $m=D_{sk}(c)=c^d \bmod n$。

从 RSA 算法实现过程可以看出，RSA 加解密变换互为逆过程，其加密过程如图 1 所示。

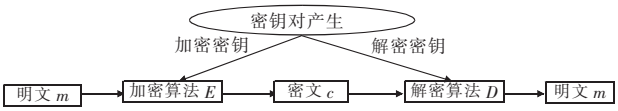

图 1 RSA 算法加密过程

假定明文 m_1、m_2，使用 RSA 算法加密后得到 $E(m_1)=m_1^e \bmod N$，$E(m_2)=m_2^e \bmod N$，其中 $E(m_1)$、$E(m_2)$ 即为加密后的密文 c_1、c_2，两者相乘得到

$$E(m_1)\times E(m_2)=(m_1^e\times m_2^e) \bmod N$$

又因为 $$E(m_1m_2)=(m_1^e\times m_2^e) \bmod N$$

所以 $$E(m_1)\times E(m_2)=E(m_1m_2)$$

由此证明 RSA 算法满足乘法同态性质。假设 RSA 密码算法的公钥为(3,5)，私钥为(3,49)。取两个明文 $m_1=13$，$m_2=14$，由 RSA 算法的乘法特性可以得到

$$E(m_1)\times E(m_2)=(m_1^e)\times(m_2^e)=3$$

$$E(m_1\times m_2)=(m_1\times m_2)^e=(13\times 14 \bmod 5)^3=3$$

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

由上述两式可知,RSA 公钥密码算法满足乘法同态特性。

RSA 算法的乘法同态特性在一定程度上协助了对 RSA 的攻击,如选择明文攻击。文献 [24] 使用 RSA 算法对密钥进行了分解,利用 RSA 算法的乘法同态特性对加密的矩阵列元素进行乘积计算,实现了多个数据的安全排序。

RSA 算法的缺陷在于公钥和私钥生成后,加密或解密中的参数固定下来,这会导致同个明文加密后的密文总是相同的,带来一定的安全性问题。后有学者提出了两种基于经典随机化的同态加密算法。

1.3.2　ElGamal 体制

ElGamal 体制是第一个基于离散对数的公钥加密体制,于 1984 年由埃及密码学家 Elgamal 提出[5],其安全性是基于离散对数问题的困难性。ElGamal 算法分为以下几个方面:

a) 密钥的产生。设 p 是一个大素数,g 是 Z_P^* 的生成元。随机选择 x,且 $1 < x < p-1$,计算 $y = g^x \bmod p$,公钥 $pk = y$,私钥 $sk = x$。

b) 加密过程。对于明文空间 Z_P^* 上的任意明文 m,随机选择 k,且 $k \in (1, p)$,加密得到密文 $c = E_{pk}(m) = (c_1, c_2)$,$c_1 \equiv g^k \pmod p$,$c_2 \equiv my^k \pmod p$。

c) 解密过程。对于任意密文 c,解密得到明文:

$$m = D_{sk}(c) = \frac{c_2}{c_1^x} = \frac{my^r}{g^{xr}} = \frac{myg^{xr}}{g^{xr}} \bmod p$$

根据上述描述步骤,可以得出 ElGamal 算法满足乘法同态。满足乘法同态的表达式为

$$E_{pk}(m_1) \times E_{pk}(m_2) = (g^{r1}, m_1 y^{r1})(g^{r2}, m_2 y^{r2}) = (g^{r1+r2}, (m_1 \times m_2) y^{r1+r2}) = E_{pk}(m_1 m_2)$$

ElGamal 算法是基于有限域上的运算,算法特点是密文由两部分组成,满足乘法同态特性。ElGamal 算法在电子投票、多方排序等领域取得了广泛应用。

1.3.3　Paillier 体制

Paillier 体制是第一个基于判定合数剩余类问题的加法同态加密密码体制,于 1999 年由学者 Paillier 提出[6],其安全性是基于判定合数剩余问题,该体制支持任意多次加法同态操作。Paillier 算法分为以下几个步骤描述:

a) 密钥生成。设 p、q 是两个满足要求的大素数,且 $N = pq$,$g \in Z_{N^2}^*$,设 $L(x) = (x-1)/N$,公钥 $pk = (N, g)$,其中 N 为公开模,而 g 为公开基。密钥 $sk = \lambda(N) = lcm(p-1, q-1)$。

b) 加密过程。对于任意明文 $m \in Z_n$,随机选择 $r \in Z_N^*$,得到密文 $c = E_{pk}(m) = g^m r^N \bmod N^2$。

c) 解密过程。对于任意密文 $c \in Z_n$,解密得到明文:

$$m = D_{sk}(c) = L(c^{\lambda(N)} \bmod N^2) / L(g)^{\lambda(N)} \bmod N^2 \bmod N$$

假定明文 m_1、m_2,分别对其进行加密操作 $E(m_1) = g^{m_1} r_1^N \bmod N^2$ 和 $E(m_2) = g^{m_2} r_2^N \bmod N^2$,得到

$$E(m_1) \times E(m_2) = g^{m_1+m_2}(r_1 r_2)^N \bmod N^2 = E(m_1 + m_2)$$

由以上表达式可知,Paillier 公钥密码体制满足加法同态特性。

1.3.4　GM 体制

1984 年,美国学者 Goldwasse 和 Micali 提出 GM 体制,该体制是第一种具有语义安全性的半同态加密方案,其安全性是基于二次剩余问题的困难性。该体制缺点为每一次加密只能处理 1 bit 信息。1994 年,学者 Benaloh 在 GM 体制的基础上提出了一种改进的概率同态加密体制,并将该方案应用于实际中。

1.3.5　BGN 体制

BGN 体制是第一种可以同时支持任意多次加法和一次乘法同态运算的方案,即能计算密文的二次函数,加密过程无密文长度扩展,且具有语义安全性。BGN 体制仅适用于二次表达式,但该体制是距全同态加密方案最近的一种体制。2010 年,学者 Gentry、Halevi 和 Vaikuntanathan 提出一种由 BGN 方案改进的体制,称为 GHV 体制,该体制安全性是基于容错问题的困难性。

问题描述如下:

输入: 假设安全参数 λ,$n = q_1 q_2$(q_1、q_2 为 λ bit 的素数),G、G_1 为 n 阶群,e: $G \times G \to G_1$ 为双线性映射,给定参数(n, G, G_1, e) 以及元素 $x \in G$。

输出: 如果 x 的阶为 q_1,则输出 1,否则输出 0。

子群判定问题的实际含义是: 当 n 的分解未知时,判定 n 阶群 G 中元素能否生成 G 的子群。在 BGN 密码的构造中,假设这个问题是困难的,即群 G 中的均匀分布与其子群中的均匀分布多项式时间不可区分。构造如下:

a) KeyGen(λ)。给定 λ,选择 λ 位 q_1、q_2(为大素数),$n = q_1 q_2$,两个 n 阶群 G、G_1,g,$u \xleftarrow{R} G$ 并令 $h = u^{q_2}$。公钥 $pk = (n, G, G_1, e, g, h)$,私钥 $sk = q_1$。

b) Enc(pk, m)。设明文空间为整数集$\{0, 1, \cdots, T\}$,$T < q_2$,m 为加密消息,$r \leftarrow \{0, 1, \cdots, n-1\}$,$C = g^m h^r \in G$,输出 C。

1.4　同态加密构造

同态加密是由四个部分组成,分别为密钥的生成、同态加密、同态解密及同态赋值。密钥的生成是由安全参数 λ 生成公钥 pk、私钥 sk。同态加密是指给出指定明文 $m \in \{0,1\}^*$,用公钥 pk 加密明文 m,得出密文 c。同态解密是指输入私钥 sk 和密文 c 进行解密运算,输出明文 m'。同态赋值是指输入公钥 pk,t 个输入的电路 C,一组密文 $c = (c_1, \cdots, c_t)$,输出 $c^* = \text{evaluate}(pk, C, c)$,且满足 $\text{dec}(sk, c^*) = C(m_1, \cdots, m_n)$。其中 evaluate 算法是完全同态加密中最重要的部分,通过 evaluate 可以对任意函数进行计算,输入都是密文,最重要的是可以计算解密函数,这是形成完全同态加密的关键。

同态加密方案既可以是对称加密方案,也可以是非对称加密方案,但一般用得多的是同态公钥加密方案即非对称加密方案,即加解密密钥不同。

2　全同态加密

2.1　研究进展

全同态加密是继 RSA 算法提出不久后由 Rivest 等人于 1978 年提出的加密方案。全同态加密方案自从被密码学界提出后,一直被誉为密码学圣杯,但是三十多年来,这个公开问题迟迟未被解决,而且人们甚至无法判断全同态加密方案是否存在。在这个探索过程中,相关学者一直没有放弃,直到 2008 年底,最好的全同态方案研究结果就是 BGN 体制,该体制可以支持无限次加法同态加密操作,但是只能支持一次乘法同态操作。2009 年,IBM 研究员 Gentry 第一次使用基于理想格构造出第一个全同态加密方案(fully homomorphic encryption, FHE),并在其博士论文中对全同态加密方案进行了详细的论述[30],发现一个具有自举性的同态加密方案可以转换为一个全同态加密方案。该方案可以支持任意深度电路的计算。所

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

谓自举性是指该同态加密方案能够处理自己的解密电路以及扩展解密电路，该方案是同态密码学上的一个里程碑，给全同态加密的研究指明了新的方向。但 Gentry 提出的方案效率很低，离实际应用还有很大的差距。同年，Dijk 等人提出了第二种全同态加密方案 DGHV[31]，该方案同样使用 Gentry 构造方案中的多个构造性工具，但不需要理想格。从 2009 至今产生了一系列全同态加密方案实现及优化，其中第一代全同态加密方案都是建立在 Gentry 思想上的构造方法[31~36]，第二代全同态加密方案是基于 LWE(learning with error) 的[37~41]。全同态算法的意义在于从根本上解决将数据信息操作委托给第三方时的保密问题，因此可以用于各种云计算。但是全同态加密算法运算复杂且密文长度和密钥长度过长，以致运算效率较低。文献[42]提出一种较快速的基于整数上的全同态加密，相比文献[31]的方案具有更短的公钥长度、更小的解密复杂度，并在文献[43]中对 Gentry 的全同态加密中的重加密技术进行了总结。文献[44]提出了整数环上的全同态加密算法。全同态加密方案中加法同态加密可应用于电子投票、有损陷门函数、隐私信息检索等，乘法同态加密可应用于 BGNO5、SYY 方案。

虽然现在国内外学者提出很多改进的全同态加密[45~51]，但这些方案均实用性不够，存在这样或那样的问题而不能有效地应用在实际云平台中，Dijk 和 Gentry 等人提出的方案实际应用中加密速度很慢，开销较大。除此之外，对密文进行任意运算的时候，需要先对密文进行重加密，而重加密技术也是逐比特进行。显然，目前提出的各种全同态加密方案效率都非常低，与实际应用有很大的差距。未来的研究领域内，如何改进全同态加密方案的执行效率成为研究的重点与难点。

2.2 全同态加密方案构造

若一个加密方案 E 对加法和乘法都具有同态性质，则称该方案 E 为一个全同态加密方案。也可描述为：decrypt_E 是方案 E 的解密算法，pk 是加密密钥，sk 是解密密钥，$f(x_1,x_2,\cdots,x_t)$ 是一个 t 元函数，则 $\text{decrypt}_E(f(c_1,c_2,\cdots,c_t),sk)=f(m_1,m_2,\cdots,m_t)$。其中加法和乘法同态如图 2 所示。

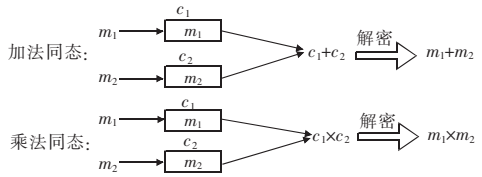

图 2 加法同态和乘法同态

一般说来，一个普通的加密方案由密码生成、加密、解密三个部分组成，而一个全同态加密方案还需要一个同态计算部分。

a) 密钥生成 KeyGen(λ)：pk 为加密密钥，sk 为解密密钥；

b) 加密 encrypt(pk,m)：用 pk 将明文加密为 c(密文)输出；

c) 解密 decrypt(sk,c)：用 sk 将密文解密为明文输出；

d) 同态计算 evaluate($pk,f,c_1,c_2,\cdots,c_t$)：输入 pk，具有 t 个输入的 f 以及 t 个密文序列 $c_1,c_2,\cdots,c_t$，其中 $c_t=\text{encrypt}(pk,m_i)\ (i=1,2,\cdots,t)$。算法的输出结果为 $c^*=\text{evaluate}(pk,f,c_1,c_2,\cdots,c_t)$，且满足 $\text{decrypt}(sk,c^*)=f(m_1,m_2,\cdots,m_t)$。

2.3 全同态加密方案分析

2.3.1 DGHV 方案

2009 年，Dijk 等人提出了 DGHV 方案，即基于整数的全同态加密方案。该加密方案在整数范围上仅仅使用了加法和乘法，只使用基本的模块化算术，并未使用理想格概念。其安全性是基于近似最大公因子问题的困难，该方案仍具有类似同态加密的操作和效率。具体实现过程如下：

a) 密钥的生成。选取一个随机的素数 p 作为密钥，且 $0<p\leqslant 2^{n^2}$。

b) 加密。选取两个随机数 q 和 r，其中 q 是一个大的正整数，且 $|2r|<q/2$，$r\sim 2^n$，$q\sim 2^{n^5}$，通过加密 1 bit 明文 $m\in\{0,1\}$，计算 $c=pq+2r+m$，得出相应的密文。

c) 解密。过程为

$$(c \bmod p) \bmod 2=[c-p(c/p)] \bmod 2=[\text{LSB}(c)] \text{ XOR } [\text{LSB}(c/p)]$$

其中：LSB(least significant bit) 表示最低有效位，因为进行模 2 运算，所以得到的结果就是该二进制数的最低位。

其同态加密特性验证如下：

设有两组明文 m_1 和 m_2，分别加密得到密文 c_1 和 c_2。其中：

$$c_1=q_1p+2r_1+m_1,c_2=q_2p+2r_2+m_2$$
$$c_1+c_2=(q_1+q_2)p+2(r_1+r_2)+m_1+m_2$$
$$c_1\times c_2=[q_1q_2p+2(r_1+m_1)+2(r_2+m_2)]p+2(r_1r_2+r_1m_2+r_2m_1)+m_1m_2$$

因为 $2(r_1+r_2)+m_1+m_2$ 远小于 p，所以

$$(c_1+c_2) \bmod p=2(r_1+r_2)+m_1+m_2$$

又因为 $2(r_1r_2+r_1m_2+r_2m_1)+m_1m_2$ 远小于 p，所以

$$(c_1\times c_2) \bmod p=2(r_1r_2+r_1m_2+r_2m_1)+m_1m_2$$

再通过模 2 运算，可得该算法满足加法同态和乘法同态特性。

2.3.2 CAFED 方案

CAFED(computing arbitrary function of encryped data) 于 2010 年由 Gentry[52] 提出。该方案将数据访问和处理分隔，在第三方不知道解密密钥的情况下也能对密文进行复杂的数据处理，实现过程如下：

首先选取一个安全参数 λ，假设 $N=\lambda$，$p=\lambda^2$，$Q=\lambda^5$。

a) 密钥的生成。选取一个随机的素数 p 作为密钥。

b) 加密。选取一个 Q 位的随机数 q，通过加密 1 bit 明文 $m\in\{0,1\}$，计算 $m'=m \bmod 2$，$c=m'+pq$。其中 m' 是一个 N 位的随机数。

c) 解密。计算 $(c \bmod p) \bmod 2$。

其同态加密特性验证如下：

设有两组明文 m_1 和 m_2，分别加密得到密文 c_1 和 c_2。其中：

$$c_1=q_1p+m_1',c_2=q_2p+m_2'$$
$$c_1+c_2=(q_1+q_2)p+m'_1+m_2'$$
$$c_1\times c_2=(q_1q_2p+q_1m_2'+q_2m_1')p+m_1'm_2'$$

因为 $m_1'+m_2'$ 远小于 p，所以

$$(c_1+c_2) \bmod p=m_1'+m_2'$$

又因为 $m_1'm_2'$ 远小于 $p/2$，所以

$$(c_1\times c_2) \bmod p=m_1'm_2'$$

再通过模 2 运算，可得该算法满足加法同态和乘法同态特性。

2.4 全同态加密方案安全性分析

2.4.1 噪声问题

在全同态加密方案中，由于公钥 p、q 是公开的，知道密文 c

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

后可以减去公钥得到 $c - pq = m + 2r$。由于存在 r 的干扰,所以无法识别明文 m,故称 $m + 2r$ 为噪声。在解密时只有当 $c \bmod p = m + 2r < p/2$ 时,再对它进行模 2 运算才能正确解密,即 $(m + 2r) \bmod 2 = m$。若噪声大于 $p/2$ 时,$c \bmod p$ 就不再等于 $m + 2r$,解密就可能不成功,所以噪声问题是影响解密的关键。而噪声会在密文计算中增长,具体情况如下:

设 $c_1 = m_1 + 2r_1 + pq_1$,$c_2 = m_2 + 2r_2 + pq_2$,得到密文加和密文乘的运算:

$$c_1 + c_2 = (q_1 + q_2)p + 2(r_1 + r_2) + m_1 + m_2$$

$$c_1 \times c_2 = [q_1 q_2 p + 2(r_1 + m_1) + 2(r_2 + m_2)]p + 2(r_1 r_2 + r_1 m_2 + r_2 m_1) + m_1 m_2$$

$$(c_1 + c_2) \bmod p = 2(r_1 + r_2) + m_1 + m_2$$

$$(c_1 \times c_2) \bmod p = (m_1 + 2r_1)(m_2 + 2r_2)$$

由上可见,密文之和的噪声是各自密文的噪声之和,密文之积的噪声是各自密文的噪声之积。由上述运算可知,噪声的主要来源还是乘法运算,在乘法运算中噪声被放大得很快。一旦超过阈值,就会使解密结果不可靠。噪声问题是实现全同态加密方案的最大障碍,如何对噪声进行控制成为全同态加密方案中的重点与难点。

2.4.2　重加密技术

全同态加密方案中的同态解密可以把在 (pk, sk) 下加密的一个密文转换为在 (pk, sk) 下加密的一个新密文,且保持消息不变,这种技术叫做重加密技术。若一个方案具有自举性,就能通过同态解密来降低密文的噪声,扩大其同态处理能力,且能处理任意复杂布尔电路。为获得自举性,Gentry 在其博士论文中引入压缩解密电路技术,降低解密算法的计算复杂度。Gentry 利用一种巧妙的 three-for-two 技术,产生辅助解密计算的预处理密文信息,但并未给出具体实现过程。2010 年,Smart 等人[32] 提出了一种相对小的密钥和密文尺寸的全同态加密方案,给出了其方案的重加密过程及噪声分析。2011 年,Gentry 等人[53] 在欧密会上给出一个全同态加密方案的实施,将重加密技术用进位加法代替 three-for-two 技术,使得解密计算的复杂度更低,更容易实现。

2.5　Gentry 全同态加密方案的对比分析

目前,对 Gentry 基于理想格的全同态加密方案在公钥生成、密钥生成以及加/解密方面进行了对比分析,结果如表 1 所示。

表 1　Gentry 全同态加密方案对比分析

方案	λ	公钥	密钥生成	加/解密
Smart-Vercauteren [32]	≈72	3.01 MB	3.2 min	N/A
DGHV [31]	≈72	2.25 GB	2.2 h	31 min
Gentry-Halevi [54]	72	λ^{10}	N/A	N/A
Coron Integer [36]	72	802 MB	43 min	14.55 min

可以看出,无论在生成方面还是在加解密方面,所耗的内存与时间相对而言比较多,而从以上几个方案对比可知,Smart-Vercauteren 方案所占用的内存与时间是相对最少的。

3　结束语

近年来,国内外学者对全同态加密方案提出了很多改进方案,但其构造方法在本质上并未有重大突破,全同态加密的发展趋于自然、简单、直观。如何改进全同态加密方案的执行效率成为未来的研究重点与难点。目前亟待解决的问题主要表现在以下几个方面: a) 如何在确保数据安全的前提下选择合适的同态加密方案实现云服务器上的密文数据高效检索; b) 如何解决全同态加密方案中存在的噪声问题、运算复杂且运算效率低问题; c) 如何在确保全同态加密方案安全性的前提下,使全同态加密方案逐步地实用化。

云计算是信息发展的核心应用,云平台上实用的全同态加密方案具有很好的理论价值和应用前景,进一步的研究应包括: a) 对 Gentry 提出的基于理想格的全同态加密方案进行理论上的深入研究; b) 开发出具有实际应用价值的全同态加密系统; c) 在已有成果的基础上,对已提出的全同态加密方案进行时间上的优化,以促进全同态加密的实践研究。

参考文献:

[1] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms [J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[2] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126.

[3] Goldwasser S, Micali S. Probabilistic encryption [J]. Journal of Computer and System Sciences, 1984, 28(2): 270-299.

[4] Cohen J D, Fischer M J. A robust and verifiable cryptographically secure election scheme [C] //Proc of the 26th Annual Symposium on Foundations of Computer Science. Washington DC: IEEE Computer Society, 1985: 372-382.

[5] Elgamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Trans on Information Theory, 1985, 31(4): 469-472.

[6] Ajtai M, Dwork C. A public-key cryptosystem with worst-case equivalence [C] //Proc of the 29th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1997: 284-293.

[7] Okamoto T, Uchiyama S. A new public-key cryptosystem as secure as factoring [C] //Advances in Cryptology. Berlin: Springer, 1998: 308-318.

[8] Naccache D, Stern J. A new public key cryptosystem based on higher residues [C] //Proc of the 5th ACM Conference on Computer and Communications Security. New York: ACM Press, 1998: 59-66.

[9] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [C] //Advances in Cryptology. Berlin: Springer, 1999: 223-238.

[10] Damgard I, Jurik M. A generalization, a simplification and some applications of Pailler's probabilistic public-key system [C] //Proc of the 4th International Workshop on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2001: 119-136.

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

[12] Regev O. On lattice, learning with errors, random linear codes and cryptography [C] //Proc of the 37th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2005: 84-93.

[13] Sander T, Young A, Yung M. Non-interactive cryptocomputing for NC^1 [C] //Proc of the 40th Annual Symposium on Foundations of Computer Science. Washington DC: IEEE Computer Society, 1999: 554-556.

[14] Boneh D, Goh E J, Nissim K. Evaluating 2-DFN formulas on ciphertexts [C] //Proc of the 2nd International Conference on Theory of Cryptography. Berlin: Springer, 2005: 325-341.

[15] Ishai Y, Paskin A. Evaluating branching programs on encrypted data

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

[C] //Proc of the 4th International Conference on Theory of Crypography. Berlin: Springer, 2007: 575-594.

[16] Gentry C, Halevi S, Vaikuntanathan V. A simple BGN-type cryptosystem from LWE [C] //Proc of the 29th International Conference on Theory and Application of Cryptographic Techniques. Berlin: Springer, 2010: 506-522.

[17] Melchor C, Gaborit P, Herranz J. Additively homomorphic encryption with *d*-operand multiplications [C] //Proc of the 30th Annual Conference on Cryptology. Berlin: Springer, 2010: 138-154.

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

[19] Diffie W, Hellman M E. New directions in cryptography [J]. IEEE Trans on Information Theory, 1976, 22(6): 644-654.

[20] Benaloh J. Dense probabilistic encryption [C] //Proc of Workshop on Selected areas of Cryptography. 1994: 120-128.

[21] Xiang Guangli, Chen Xinmeng, Ma Jie, *et al*. Homomorphic encryption scheme in the range of the real [J]. Computer Engineering and Applications, 2005, 41(20): 12-14.

[22] 肖倩, 罗守山, 陈萍. 半诚实模型下安全多方排序问题的研究 [J]. 电子学报, 2008, 36(4): 709-714.

[23] 邱梅, 罗守山, 刘文. 利用 RSA 密码体制解决安全多方多数据排序问题 [J]. 电子学报, 2009, 37(5): 1119-1123.

[24] 黄福人. 电子投票的研究与设计 [D]. 合肥: 中国科学技术大学, 2010.

[25] 张鹏, 喻建平, 刘宏伟. 同态签名方案及其在电子投票中的应用 [J]. 深圳大学学报: 理工版, 2011, 28(6): 489-494.

[26] 李美云, 李剑, 黄超. 基于同态加密的可信云存储平台 [J]. 信息网络安全, 2012(9): 35-40.

[27] Li Jian, Chen Sicong, Song Danjie. Security structure of cloud storage based on homomorphic encryption scheme [C] //Proc of the 2nd International Conference on Cloud Computing and Intelligent Systems. Washington DC: IEEE Computer Society, 2012: 224-227.

[28] 彭长根, 田有亮, 张豹, 等. 基于同态加密体制的通用可传递签名方案 [J]. 通信学报, 2013, 34(11): 18-25.

[29] 杨玉龙, 彭长根, 周洲. 基于同态加密的防止 SQL 注入攻击解决方案 [J]. 信息网络安全, 2014(1): 30-33.

[30] Gentry G. A fully homomorphic encryption scheme [D]. Stanford: Stanford University, 2009.

[31] Van Dijk M, Gentry C, Halevi S. Fully homomorphic encryption over the integers [C] //Advances in Cryptology. Berlin: Springer, 2010: 24-43.

[32] Smart N P, Vercauteren F. Fully homomorphic encryption with relatively small key and cipher sizes [C] //Proc of the 13th International Conference on Public Key Cryptography. Berlin: Springer, 2010: 420-443.

[33] Stehle D, Steinfeld R. Faster fully homomorphic encryption [C] // Proc of the 16th International Conference on Theory and Application of Cryptographic and Information Security. Berlin: Springer, 2010: 377-394.

[34] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages [C] //Proc of the 31st Conference on Advances in Cryptology. Berlin: Springer, 2011: 505-524.

[35] Coron J S, Naccache D, Tobouchi M. Public key compression and modulus switching for fully homomorphic encryption over the integers [C] //Proc of the 31st International Conference on Theory and Application of Cryptographic Techniques. Berlin: Springer, 2012: 446-464.

[36] Coron J S, Mandal A, Naccache D. Fully homomorphic encryption over the integers with shorter public keys [C] //Proc of the 31st International Conference on Advances in Cryptology. Berlin: Springer, 2011: 487-504.

[37] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE [J]. SIAM Journal on Computing, 2014, 43(2): 831-871.

[38] Brakerski Z, Gentry C. Fully homomorphic encryption without bootstrapping [C] // Proc of the 3rd Innovations in Theoretical Computer Science Conference. New York: ACM Press, 2012: 309-325.

[39] Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP [C] //Proc of the 32nd Cryptology Conference. Berlin: Springer, 2012: 868-886.

[40] Lopen-Alt A, Tromer E, Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption [C] //Proc of the 44th Symposium on Theory of Computing. New York: ACM Press, 2012: 1219-1234.

[41] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: conceptually-simper, asymptotically-faster, attribute-based [C] //Proc of the 33rd Annual Cryptology Conference. Berlin: Springer, 2013: 75-92.

[42] Tang Dianhua, Zhu Shixiong, Cao Yunfei. Faster fully homomorphic encryption scheme over integer [J]. Computer Engineering and Application, 2012, 48(28): 117-122.

[43] 汤殿华, 祝世雄, 曹云飞. 整数上的全同态加密方案的重加密技术 [J]. 信息安全与通信保密, 2012(1): 76-79.

[44] 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.

[45] 汤殿华, 祝世雄, 王林, 等. 基于 RLWE 的全同态加密方案 [J]. 通信学报, 2014, 35(1): 173-182.

[46] 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.

[47] 于志敏, 古春生, 景征骏. 基于整数近似 GCD 的全同态加密方案 [J]. 计算机应用研究, 2014, 31(7): 2105-2108.

[48] 陈智罡, 王箭, 宋新霞. 全同态加密研究 [J]. 计算机应用研究, 2014, 31(6): 1624-1631.

[49] 汤全有, 马传贵. 针对全同态加密体制的反馈攻击 [J]. 计算机工程, 2014, 40(6): 79-84.

[50] Li Jian, Song Danjie, Chen Sicong, *et al*. A simple fully homomorphic encryption scheme available in cloud computing [C] //Proc of the 2nd IEEE International Conference on Cloud Computing and Intelligent Systems. Washington DC: IEEE Computer Society, 2012: 214-217.

[51] 光炎, 祝跃飞, 顾纯祥, 等. 一种针对全同态加密体制的密钥恢复攻击 [J]. 电子与信息学报, 2013, 35(12): 2999-3004.

[52] Gentry C. Computing arbitrary functions of encrypted data [J]. Communications of the ACM, 2010, 53(3): 97-105.

[53] Gentry C, Halevi S. Implementing Gentry's fully-homomorphic encryption scheme [C] //Advances in Cryptology. Berlin: Springer, 2011: 129-148.

[54] Gentry C, Halevi S. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits [C] //Proc of the 52nd IEEE Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 2011: 107-109.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net