Software Engineering and Applications 软件工程与应用, 2013, 2, 43-46
http://dx.doi.org/10.12677/sea.2013.22008 Published Online April 2013 (http://www.hanspub.org/journal/sea.html)

A Proof Based on the Somewhat Homomorphic Encryption Scheme*

Jing Yang[1], Mingyu Fan[1], Guangwei Wang[1], Zhiyin Kong[2]

[1]University of Electronic Science and Technology of China, Chengdu
[2]Science and Technology on Information Assurance Laboratory, Beijing
Email: ay4922@163.com

Received: Feb. 4th, 2013; revised: Feb. 19th, 2013; accepted: Mar. 1st, 2013

Abstract: In the Gentry's Homomorphic encryption scheme, Somewhat homomorphic encryption is the base of Gentry's homomorphic encryption. For the present study is based on the most Somewhat homomorphism encryption scheme to develop without Somewhat homomorphism encryption scheme proof, this paper gives a proof based on Somewhat homomorphism encryption scheme.

Keywords: Somewhat Homomorphic Encryption; Homomorphism; Decryption

基于 Somewhat 同态加密方案的一种证明*

杨　竞[1]，范明钰[1]，王光卫[1]，孔志印[2]

[1]电子科技大学计算机学院，成都
[2]信息保障技术重点实验室，北京
Email: ay4922@163.com

收稿日期：2013 年 2 月 4 日；修回日期：2013 年 2 月 19 日；录用日期：2013 年 3 月 1 日

摘　要：在 Gentry 的同态加密理论中，Somewhat 同态加密是 Gentry 框架中的全同态加密方案的基础。由于目前的研究多数是基于 Somewhat 同态加密方案的拓展而少有对 Somewhat 同态加密方案的证明，本文给出基于 Somewhat 同态加密方案的一种证明。

关键词：Somewhat 同态加密；同态性；解密

1. 引言

目前，云计算有着巨大的发展前景，云计算的应用已经成为企业和政府的一种趋势。但是云计算的应用存在巨大的瓶颈，那就是云计算的安全问题[1]。在云背景下，为了保障安全，云服务商需要对用户加密后的数据进行操作，但是如果采用传统的密码算法，必须先解密用户加密的明文，才能进行云计算处理。而采用同态加密算法，可以对用户加密后的数据进行操作而不用先解密，这样就可以解决云计算的安全问题。

1978 年 Rivest，Adleman 和 Dertouzos[2]提出了“秘密同态”的概念，即一种算法可以像对明文一样对密文进行各种计算。Rivest 等人给出了同态加密方案的 4 个算法。Rivest 方案满足加法和乘法的同态，小数据加密问题，能够抵御已知明文攻击和已知密文攻击。

在 Rivest 等人提出“秘密同态”的概念之后，国

*资助信息：受信息保障技术重点实验室(Science and Technology on Information Assurance Laboratory)开放基金资助。

内外学者对同态加密进行了大量的研究[3]，但所提出的方案均不能做到同态计算任意深度电路或任意次数多项式处理[4]，全同态加密是密码学者多年来一直期望解决的问题。全同态加密能够在没有密钥的条件下，对加密数据进行任意复杂的操作，以实现相应的明文操作。直到 2009 年，Gentry[5,6]基于理想格提出了第一个全同态加密方案，并在他的博士论文中对全同态加密做了详尽的研究，解决了这个困扰密码学界 30 年的问题。

Gentry 提出的思路由以下三个方面组成：

1) 提出了自举性的思想，所谓自举性，是指一个同态方案能够同态处理自己的解密电路以及扩展解密电路。由于加密中噪声的存在(本文的 4.1 有关于噪声的定义和描述)，加法同态和乘法同态会使噪声增加，因此方案的同态处理能力是有限的。如果方案具有自举性，就可以通过同态解密来降低密文的噪声，扩大其同态处理能力，以致能够处理任何复杂的布尔电路。

2) 描述了一个具有自举性，使用理想格的公钥加密理论。基于格的密码体系在加密算法上有低电路复杂度，理想格提供了加法同态和乘法同态。

3) 引入了“压缩解密电路”的技术，降低解密算法的计算复杂度。该技术产生了辅助解密计算的预处理密文信息的技术。

在文献[7]中，对 Gentry 方案的证明了在整数环上的全同态加密算法。由于现在文献多数在于阐述 Gentry 的方案而很少给出详细证明，本文给出 Somewhat 同态加密方案的解密正确性和同态性的一种证明。

2. 相关定义

2.1. 同态

设 R 表示明文空间，S 表示密文空间。$a,b\in R$，E 是 $R\to S$ 上的加密函数，如果存在算法 $\oplus$ 和 $\otimes$，使其满足：

$$E(a+b)=\oplus\left(E(a),E(b)\right) \tag{1}$$

$$E(a\times b)=\otimes\left(E(a),E(b)\right) \tag{2}$$

我们可以利用 $E(a)$ 和 $E(b)$ 的值计算出 $E(a+b)$ 和 $E(a\times b)$，而不需要知道 a,b 的值。我们称满足式(1)的算法为满足加法同态，满足式(2)的算法为满足乘法同态。

2.2. 最近整数

对于只有一个整数位的有理小数 $e=(e_0e_{-1}e_{-2}e_{-3}\cdots)_2$，即 $e=e_0+2^{-1}e_{-1}+2^{-2}e_{-2}+\cdots$ 则 $\lfloor e\rceil \bmod 2=(e_0+e_{-1})\bmod 2$，用符号 $\lfloor e\rceil$ 表示取最近整数，即 $\lfloor e\rceil\in(e-1/2,e+1/2]$。

3. Somewhat 同态加密方案

在 Gentry[3,5,6]的框架中，Somewhat 同态加密方案是全同态加密方案的基础，记为：

$SHE=(keygen,Enc,Dec,Evaluate)$，由以下几个部分组成：

参数选取：$\rho=\lambda$，$\rho'=2\lambda$，$\eta=\tilde{\mathrm{O}}(\lambda^2)$，$\theta=\tilde{\mathrm{O}}(\lambda^4)$，$\gamma=\tilde{\mathrm{O}}(\lambda^5)$，其中：$\lambda$ 为安全参数。安全参数与方案的安全性相关，通常取几十到几百比特。

$keygen$：随机选择 η 比特的奇素数 p 和 θ 比特的奇素数 q，令 $N=pq$。然后选取两个随机整数 $l\in[0,2^{\gamma}/p]$，$h\in(-2^{\rho},2^{\rho})$。并计算

$$x=pl+2h \tag{3}$$

设置公钥 $pk=(N,x)$，私钥 $sk=p$。

$Enc(pk,m)$：给定消息 $m\in\{0,1\}$。选择两个随机整数 $r_1\in(-2^{\rho'},2^{\rho'})$ 和 $r_2\in(-2^{\rho},2^{\rho})$，根据公钥 $pk=(N,x)$。计算

$$c=m+2r_1+r_2x \bmod N \tag{4}$$

c 作为密文输出。

$Dec(sk,c)$：根据给定的密文 c，利用私钥 sk 计算

$$m'=(c \bmod p)\bmod 2 \tag{5}$$

$Evaluate(pk,C,c_1,c_2,\cdots,c_t)$：给定一个具有 t 输入的布尔电路 C 和 t 个密文 c_i，将电路中的加法门和乘法门替换成整数上模 N 的加法门和乘法门。将 t 个密文输入到扩展的电路中执行其所有操作，输出电路的结果 $c^*=Evaluate(pk,C,c)$，验证其是否满足 $Dec(sk,c^*)=C(m_1,m_2,\cdots,m_t)$。

4. SHE 方案的一种证明

证明包括了两个部分，分别是解密正确性证明和

同态正确性证明。下面就从这两个方面进行证明。

4.1. 解密正确性证明

1) 由加密算法 $Enc(pk,m)$ 中的式(4)，将 $N=pq$ 带入其中，可得：

$$c=m+2r_1+r_2x \bmod pq \tag{6}$$

2) 将 $x=pl+2h$ 带入式(6)中，得

$$c=m+2r_1+r_2(pl+2h) \bmod pq \tag{7}$$

继续化简，得：

$$c=m+2r_1+(r_2pl+2r_2h) \bmod pq \tag{8}$$

3) 根据模的定义，我们可知存在一个 k，使得

$$a \bmod b=a+kb \tag{9}$$

由式(9)我们可得：

$$(r_2pl+2r_2h) \bmod pq=r_2pl+2r_2h+kpq \tag{10}$$

代式(10)入式(8)，有：

$$c=m+2(r_1+r_2h)+p(r_2l+kq) \tag{11}$$

4) 设 $c \bmod p$ 取值在 $(-p/2,p/2]$ 之间，则有：

$$c \bmod p=c-p\lfloor c/p \rceil \tag{12}$$

而 $\lfloor c/p \rceil$ 事实上是求 c 除以 p 的整数商，由步骤 3 最终化简得到的式(11)再除以 p：

$$\frac{c}{p}=\frac{m+2(r_1+r_2h)}{p}+(r_2l+kq) \tag{13}$$

由式(13)，可知整数商即 r_2l+kq。

5) 为了使得 $\lfloor c/p \rceil=r_2l+kq$，我们必须要求 $\left|\frac{m+2(r_1+r_2h)}{p}\right|<\frac{1}{2}$ 这时

$$c-p\lfloor c/p \rceil=m+2(r_1+r_2h) \tag{14}$$

6) 再对式(14)进行模 2 运算，明文就可以正确地恢复了。我们定义下面式 $m+2(r_1+r_2h)$ 称为噪声。所以，当噪声的绝对值小于 2 时，就可以正确的解密。

4.2. 同态正确性证明

在 Gentry 的同态框架中，在电路内部中各个节点更新着密文，使得密文的噪声在允许范围内，电路的每一层都保证了噪声可控，任意深度的电路或多项式都可以被同态处理。为了能够更新密文，就需要方案能够同态处理其解密电路以及扩展的解密电路。下面对 somewhat 同态方案进行同态正确性证明。

1) 设两个明文为 m_0 和 m_1，分别对其用 Somewhat 同态加密方案进行加密：

$$c_i=m_i+2r_{1i}+r_{2i}x \bmod N,\ i=0,1 \tag{15}$$

在解密正确性的步骤 2 我们已知存在整数 k_0 和 k_1 使得

$$c_i=m_i+2(r_{1i}+hr_{2i})+r_{2i}lp+k_ipq,\ i=0,1 \tag{16}$$

2) 再进行加运算

$$\begin{aligned}c_0+c_1=&m_0+m_1+2(r_{10}+hr_{20}+r_{11}+hr_{21})\\&+(r_{20}l+k_0q+r_{21}l+k_1q)p\end{aligned} \tag{17}$$

可见满足：

$$Enc(m_0)+Enc(m_1)=\oplus(Enc(m_0),Enc(m_1))$$

其中 $Enc(m_i)=c_i,\ i=0,1$。噪声变化为：

$$\begin{aligned}&|m_0+m_1+2(r_{10}+hr_{20}+r_{11}+hr_{21})|\\&\le|m_0+2(r_{10}+hr_{20})|+|m_1+2(r_{11}+hr_{21})|\end{aligned} \tag{18}$$

3) 再对 c_0 和 c_1 进行乘法运算，可以简要表示乘法结果为

$$c_0\times c_1=m_0\times m_1+2A+Bp \tag{19}$$

可见满足 $Enc(m_0)\times Enc(m_1)=\otimes(Enc(m_0),Enc(m_1))$，其中 $Enc(m_i)=c_i,\ i=0,1$。噪声变化为：

$$|m_0\times m_1+2A|\le|m_0+2(r_{10}+hr_{20})|\cdot|m_1+2(r_{11}+hr_{21})| \tag{20}$$

4) 由式(18)可见噪声在加法运算中是线性增长的，而由式(19)可见噪声乘法运算中是平方增长的，所以对方案的评估能力主要在于电路乘法深度或多项式深度。

通过上述对于 Somewhat 同态加密方案的解密正确性和同态正确性的验证，证明了 Somewhat 同态加密方案在解密和同态性的正确性。

5. 结语

同态加密方案在 1978 年由 Rivest 等人提出到 2009 年 Gentry 提出基于理想格的同态加密方案，经历了 30 多年的时间。自 Gentry 提出了 Somewhat 同态加密方案，学术界对其进行了大量的研究，但是都

是对于 Somewhat 同态加密方案的表述，而少有验证。我们通过整理已有的 Somewhat 同态加密方案的资料，对于 Somewhat 同态加密方案的解密正确性和同态性进行了证明，并给出了证明的详细步骤。

参考文献 (References)

[1] 冯登国, 张敏, 张妍等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83.

[2] R. L. Rivest, L. Adleman and M. L. Deaouzos. On data banks and privacy homomorphism. In R. A. DeMillo, Ed., Foundations of secure computation. New York: Academic Press, 1978: 169-179.

[3] J. Domingo-Ferrer. A provably secure additive and multiplicative privacy homomorphism. In Proceedings of the 5th International Conference on Information Security. Berlin: Springer-Verlag, 2002: 471-483.

[4] N. P. Smart. 密码术与编码[M]. 武汉: 湖北辞书出版社, 2008: 126-128.

[5] C. Gentry. A fully homomorphic encryption scheme. Stanford: Stanford University, 2009.

[6] G. Gentry, S. Halevi. Implementing Gentry's fully homomorphic encryption scheme. Advances in Cryptology-EUROCRYPT 2011 Lecture Notes in Computer Science, 2011, 6632: 129-148.

[7] 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, 24: 1-4.