

一种适用于云计算环境的改进全同态加密方案

锡晓峰, 曹宝香

(曲阜师范大学 计算机科学学院, 山东 日照 276826)

摘要:针对云计算环境中数据的安全性要求,在现有的全同态加密方案的研究基础上,提出了一种改进的全同态加密方案。改进的全同态加密方案在 DGHV 方案基础上同时结合将模 2 运算变为模 4 运算、减小公钥尺寸和引入一个比较大的固定数的方法,构成了更适合云计算环境的改进全同态加密算法。改进的全同态加密方案具有公钥尺寸小、一次加密 2 bit 密文和密文检索时不需要将私钥暴露给服务器的特点。文中对改进的全同态加密方案与 DGHV 全同态加密方案在密文检索方面进行了比较。最后提出了全同态加密方案在云计算环境中的适用场景。

关键词:云计算;全同态加密;隐私数据检索;数据安全

中图分类号:TP301

文献标识码:A

文章编号:1673-629X(2015)02-0144-04

doi:10.3969/j.issn.1673-629X.2015.02.033

An Improved Fully Homomorphic Encryption Scheme under Conditions of Cloud Computing

XI Xiao-feng, CAO Bao-xiang

(College of Computer Science, Qufu Normal University, Rizhao 276826, China)

Abstract:For data security requirements under the conditions of cloud computing, propose an improved fully homomorphic encryption scheme based on the existing research of fully homomorphic encryption scheme. The improved fully homomorphic encryption scheme is based on the DGHV scheme and combined with the method which changes mode 2 operation into mode 4 operation, and reduces the size of the public key, and introduce a relatively large number of fixed, forming the improved fully homomorphic encryption algorithm is more suitable for a cloud computing environment. This scheme has advantages in public key with a small size, encryption 2bit one time and without exposing the private key to the server. The improved fully homomorphic encryption scheme is compared with DGHV fully homomorphic encryption scheme in the ciphertext retrieval. Finally, propose the applicable scenes of fully homomorphic encryption scheme under the conditions of cloud computing.

Key words:cloud computing; fully homomorphic encryption; private data retrieval; data security

0 引言

云计算应用越来越广泛,同时云计算的安全问题也暴露的越来越严重。2013 年 6 月,美国国家安全局(NSA)窃取数据的秘密文件的曝光(即棱镜门事件),让人们对于存储在云端数据的安全性产生怀疑。此事件直接导致美国云计算供应商损失 10%~20% 的市场占有率。云计算让数据控制和存储环境发生了改变,所有的数据被放在了一个开放的大环境里,没有了防火墙等隔离设施的保护。数据如果得不到有效保护,则会轻易地被窃取和泄露。人们对自己数据的安

全意识逐渐增强,数据加密是数据安全一个比较好的解决方案。

1 全同态加密

在 20 世纪 70 年代,Rivest 等首先提出了同态加密这类特殊的自然加密方法^[1],但是所提出的同态加密算法只满足加法同态和乘法同态。由于当时的同态加密算法不仅不能适应所有计算操作的需求,而且有的效率非常低,有的非常容易破解,所以同态加密算法一直没有得到现实应用。

这种状况直到 2009 年得到了改善,IBM 的克雷格

收稿日期:2014-03-19

修回日期:2014-06-25

网络出版时间:2014-12-27

基金项目:山东省科技发展计划资助项目(2012GGX10123)

作者简介:锡晓峰(1987-),女,硕士研究生,研究方向为企业信息化与系统集成、云计算数据安全;曹宝香,教授,研究方向为企业信息化与系统集成、云计算。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20141227.1347.040.html>

金特里(Craig Gentry)发现了一种全新的同态加密方案。这种方案是基于理想格的全同态加密方案。该方案因为支持所有运算操作所以被称为全同态^[2]。虽然这个方案给后续研究带来了突破性进展,但是该方案由于加解密效率低下而没有得到实际应用。

Dijk 等^[3]在 2010 年提出基于模运算的整数全同态方案(又称 DGHV 算法),但是方案的执行效率低下,并且公钥拥有的尺寸太大。Smart 等^[4]基于 Gentry 等的全同态加密方案,提出具有较高效率的、拥有较小密钥和密文尺寸的全同态加密方案。Jean 等在 2011 年对 DGHV 算法进行了改进,改变了 DGHV 算法不能对明文序列加密的缺点,并且给出了语义安全的证明^[5]。

加密方法对密文的计算操作可以直接对应到解密生成明文的计算操作,因此在现实中使用广泛。例如在电子竞拍^[6]、投票选举等方面的应用。

1.1 同态加密原理

同态加密又称为秘密同态,秘密同态技术的概念是建立在代数理论基础上的,Gentry 等提出的全同态概念可以描述为^[2]:

假设加密函数为 EK、解密函数为 DK、运算操作为 α 和明文 $M(m_0, m_1, \dots, m_i)$, 公式为

$$\alpha(DK(M(m_0, m_1, \dots, m_i))) = D(\alpha(M(m_0, m_1, \dots, m_i)))$$

一个全同态方案由四种算法组成:

密钥部分(Key):根据给出的参数 γ 生成公钥 pk 和私钥 sk;

加密部分(Enc):用公钥 pk 加密明文 M 得到加密后的密文 C ;

解密部分(Dec):用私钥解密密文 C 得到明文 M ;

额外评估部分(Evaluate):输出 t 个输入的电路 C (由 mod2 加法门和乘法门组成)和公钥 pk,还有明文对应的密文 c 。用公式可以表示成输出为 Evaluate(pk, C, c)。

1.2 DGHV 全同态加密

DGHV 的具体方案为^[3]:

(1) 构造一个 somewhat 加密方案。

生成密钥:选取 p 作为密钥,其中 p 满足的条件为: p 是一个大素数且 $p \in [2^{\gamma-1}, 2^{\gamma})$;

加密部分:1 bit 的明文 $m \in \{0, 1\}$, m 加密生成的密文 $c = m + pq + 2r$, q 和 r 是在加密过程中随机生成的,其中 q 是一个较大的整数且要远大于 p , r 是一个较小的整数且 $2r$ 小于 p 的一半;

解密部分:解密过程为明文 $m = (c \bmod p) \bmod 2$ 。

(2) 在对称的 somewhat 方案基础上构造一个非对称方案。

由于 q 是对外开放的,那么如果 pq 作为公钥,很容易计算出私钥 p 的值,所以假设一个集合 $\{x_i, x_i = pq_i + 2r_i\}$,选择集合中的任意项构成子集 S ,将子集中元素的和作为公钥 $\text{sum}(s) = \sum x_i$,构成的 DGHV 方案的加密操作可用式子表示为: $c = m + 2r + \text{sum}(s)$ 。使用 $\text{sum}(s)$ 作为公钥,即使攻击者能窃听到某个 x_i ,仍然很难破解出 p 。

(3) 利用自举性对构造的方案去除噪音。

由解密公式可以知道,当密文 $c \bmod p(\frac{p}{2}, \frac{p}{2})$ 时,解密能保证是得到正确的明文。如果超出这个范围则解密是错误的。重加密过程为每次进行密文操作前,对“新鲜”密文,实行一次加密操作,从而使每次要进行加法和乘法等计算操作的密文保持“新鲜”,从而达到消减噪音的目的。这样得到的方案就可以对密文无限地进行计算操作,达到所说的全同态。

2 改进的基于整数的全同态加密方案

文献[5]中,Jean 等提出了一种改进的全同态加密方案(BDGHV)。BDGHV 方案支持批处理,能同时对多个字符进行加密,但是加密过程中生成的公钥还是很长。文献[7]中分析,如果 BDGHV 方案能抵御格攻击,那么公钥至少为 2^{46} 位。这么大的公钥长度在实际应用中是无法真正实现的,所以在综合以上全同态加密的基础上,提出了一种更加适合云计算平台的可搜索加密算法。

2.1 改进方案原理及实现

在文献[8-9]的基础上,提出一种能一次加密 2 比特密文,公钥更小,更适合云计算的基于 DGHV 方案的全同态加密算法。文献[10]在 DGHV 方案基础上提出了称为 SDC 的算法。

笔者在这些算法基础上提出一种安全性不低于 DGHV 方案的全同态加密算法。

对文中使用的符号进行说明:

λ :安全参数;

ρ :噪声长度,为抵抗暴力攻击 $\rho = \omega(\log \lambda)$;

η :私钥二进制长度, η 满足 $\eta \geq \rho \Theta(\lambda \log^2 \lambda)$,这样才能保证压缩解密可行;

γ :公钥二进制长度,为抵抗格攻击, $\gamma = \omega(\eta^2 \log \lambda)$;

τ :公钥个数, $\tau \geq \gamma + \omega(\log \lambda)$,文中需要的公钥个数为 $2\sqrt{\tau}$ 。

其中 $\omega()$ 是高阶无穷大量。

使用 DGHV 方案的框架构造全同态加密方案:

首先,构造部分同态的 somewhat 方案:将模 2 运

算改为模4运算,使得一次能加密2 bit的密文,令 λ 为安全参数。

(1) KeyGen(λ):由安全参数 λ 生成 η 比特的密钥 p 。

(2) Encrypt(sk, m):对 $m \in \{00, 01, 10, 11\}$ 进行加密得 $c = m + 4r + pq$,其中, r 是随机生成 p 的整数, r 是加密过程中随机生成的 γ 比特的整数。

(3) Decrypt(sk, c): $m = (c \bmod p) \bmod 4$ 。

$c \bmod p$ 的值为噪声,也就是说只有 $m + 4r < \frac{p}{2}$ 时,

$c \bmod p = m + 4r$,则这时得到的解密后的结果是正确的。由安全参数知,只要是“新鲜”密文,永远成立。对方案的同态性进行验证:

$$c_1 = m_1 + 4r_1 + pq_1$$

$$c_2 = m_2 + 4r_2 + pq_2$$

$$[(c_1 + c_2) \bmod p] \bmod 4 = [m_1 + m_2 + 4(r_1 + r_2)] \bmod 4 = m_1 + m_2$$

$$[(c_1 * c_2) \bmod p] \bmod 4 = [m_1 m_2 + 4(m_2 r_1 + 4r_1 r_2 + m_1 r_2)] \bmod 4 = m_1 m_2$$

很明显密文是“新鲜”的,所以密文加法和乘法是满足同态性的,但是在不断的运算操作中产生的噪音就越来越大。

其次,在 somewhat 基础上扩展到公钥方案,使用文献[9]的方法减小公钥尺寸,使用文献[11]的方法使得方案不需要将密钥暴露给服务器,从而使方案更适合云平台这个开放环境。方案步骤为:

(1) KeyGen(λ):加密过程随机生成 η 比特的私钥 p ,令 $x_0 = pq_0$,且 x_0 是奇数并符合 $r_p(x_0)$ 被4整除。按 somewhat 方案生成 $2\sqrt{\tau}$ 个0加密生成的密文: $b \in \{0, 1\}, 1 \leq i \leq \sqrt{\tau}, x_{i,b} = pq_{i,b} + 4r_{i,b}$

最终公钥尺寸为 $2\sqrt{\tau}$, $pk = \langle x_0, x_{1,0}, x_{1,1}, x_{2,0}, x_{2,1}, \dots, x_{\sqrt{\tau},0}, x_{\sqrt{\tau},1} \rangle$ 。

(2) Encrypt(pk, m): τ 维向量 $b = \langle b_{i,j} \rangle (1 \leq i, j \leq \sqrt{\tau}, b_{i,j} \in \{0, 1\})$,随机生成固定的大素数 Q , (p 的位数大于 Q 的位数)明文 $m \in \{00, 01, 10, 11\}$,密文 c 为:

$$c = (m + 4r + p + 4Q \sum_{1 \leq i,j \leq \sqrt{\tau}} b_{i,j} x_{i,0} x_{j,1}) \bmod x_0$$

(3) Decrypt(sk, c):对密文解密的明文为 $m = (c \bmod p) \bmod 4$,在加密过程中对 x_0 求模是降低密文大小。

由于改进的过程引入的 p 和 Q 这两项并没有影响到整个过程产生的噪音,过程步骤可以参考文献[8]。即使用一部分私钥信息加入公钥中,并用这部分私钥信息对密文进行预处理,密文经过预处理后解密速度会大大加快,降低了解密复杂性。

2.2 改进方案安全性分析

该方案与 DGHV 方案类似,都是最大公约数问题(GCD)。也就是针对该方案的攻击都可以转换为最大公约数问题,目前最大公约数是不可解的,所以该方案符合安全性。同时文中的压缩方法引入稀疏子集和问题,对于稀疏子集和问题可以参考文献[12],更加保证了文中算法的安全性。

2.3 改进方案与 DGHV 方案在检索方面的比较

DGHV 方案的检索过程为:

(1)将检索的关键词用 DGHV 加密算法加密得到 $c_i = m_i + 2r + p_1 q_1$, c_i 为检索关键字生成的密文。

(2)将生成的密文发送到服务器,然后服务器读取存储的密文 c 。

(3)服务器使用算法 $R = ((c - c_i) \bmod p) \bmod 2$,如果 $R=0$,则做比较的密文就是要检索的密文。

由 DGHV 方案检索的过程可以看到,如果要进行检索需要将 p 上传到服务器,也就是把 p 暴露给服务器。当服务器获取到 p 后,如果被别有用心的人看到,破坏者使用暴露的 p 就可以对密文进行解密,加密失效。

改进算法的数据检索过程:

(1)将检索的关键词用改进的加密算法加密得到:

$$c_j = (m_j + 4r_j + p + 4Q \sum_{1 \leq i,j \leq \sqrt{\tau}} b_{i,j} x_{i,0} x_{j,1}) \bmod x_0$$

其中, c_j 为检索关键字生成的密文。

(2)将生成的密文发送到服务器,然后服务器读取存储的密文 c 。

(3)服务器使用算法 $R = (c - c_j) \bmod Q$,如果 $R=0$,则做比较的密文就是要检索的密文。

在改进方案中,只需要将 Q 上传到服务器即可,把 $4 \sum_{1 \leq i,j \leq \sqrt{\tau}} b_{i,j} x_{i,0} x_{j,1}$ 作为公钥,即使获取 Q 也无法获取密钥 p 。

3 改进方案在云计算环境中的应用场景

对云中数据采用全同态加密后,可以直接从加密后的密文中提取有用信息。同时全同态加密支持密文检索,当检索时,直接在密文基础上检索出想要的信息,然后直接对这些信息进行解密,这样就大大提高了效率,减少了计算的复杂度。

全同态加密方案为:

首先,用户访问云端,密钥生成器产生公钥和私钥,并将产生的密钥通过安全通道发送给用户,用户使用其公钥加密私钥并将加密后的密钥保存在云端。其次,用户使用密钥对要加密的数据在客户端执行加密

操作。最后,用户将加密后的密文分类保存在云端,如图1所示。

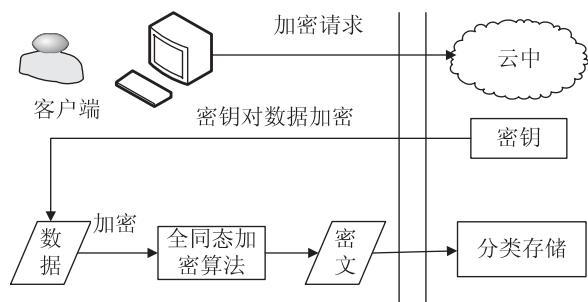


图1 用全同态加密算法加密数据

该数据安全策略适用场景为以下3个方面^[13]:

(1) 隐私保护。

用户数据以密文的形式传输并保存在云端,既保证了数据在传输过程中的安全性,又确保数据的存储安全,即便是云计算服务提供商的工作人员也无法轻易获取明文信息。

(2) 密文检索。

基于全同态加密技术的密文检索方法直接使用密文关键字对密文进行检索,保证了服务器不能获取任何检索信息,方便用户的同时也拥有较高的安全性和较强的使用性。

(3) 密文数据处理。

该方案使用同态加密可以使用户在不损害别人隐私的情况下直接在密文的基础上进行运算,从而获取用户想要的有用信息。

4 结束语

文中在 DGHV 和基于 DGHV 的一系列全同态加密算法基础上,提出了一种改进的全同态加密算法。虽然改进的全同态加密算法对公钥尺寸等进行了改进,但是由于全同态加密算法真正实现比较复杂,所以以后需要进一步的研究。

参考文献:

- [1] Rivest R L, Adleman L, Detrouzos M L. On data banks and privacy homomorphism [C]//Proc of foundations of secure computation. New York: Academic Press, 1978: 169-179.
- [2] Gentry C. A fully homomorphic encryption scheme [D]. Stanford: Stanford University, 2009.
- [3] van Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [C]//Proceedings of EUROCRYPT 2010. Riviera, French: [s. n.], 2010: 24-43.
- [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. Berlin: Springer-Verlag, 2010: 420-443.
- [5] Jean-Sebastien C, Mandal A, Nacache 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: Springer-Verlag, 2011: 487-504.
- [6] 刘 良, 蒋天发. 同态加密技术及其在物联网中的应用研究 [J]. 信息网络安全, 2011(5): 61-64.
- [7] 张 爽, 杨亚涛. 基于整数的全同态加密体制的研究 [J]. 北京电子科技学院学报, 2013, 21(2): 29-34.
- [8] 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.
- [9] Coron J S, Lepoint T, Tibouchi M. Batch fully homomorphic encryption over the integers [R]. [s. l.]: [s. n.], 2013.
- [10] Li Jian, Song Danjie, Chen Sicong, et al. A simple fully homomorphic encryption scheme available in cloud computing [C]//Proceedings of 2012 IEEE 2nd international conference on cloud computing and intelligence systems. Hangzhou: IEEE, 2012: 214-217.
- [11] 宋丹劼. 基于同态加密的云存储系统设计与实现 [D]. 北京: 北京邮电大学, 2013.
- [12] Nguyen P Q, Stern J. Adapting density attacks to low weight knapsacks [C]//Proc of Asiacrypt'05. Heidelberg: Springer-Verlag, 2005: 41-58.
- [13] 任福乐, 朱志祥, 王 雄. 基于全同态加密的云计算数据安全方案 [J]. 西安邮电大学学报, 2013, 18(3): 92-95.

2014 中国计算机学会颁奖大会

责任 创新 奉献

中国计算机学会定于2015年1月31日16:30-20:30,在北京金隅喜来登酒店大宴会厅举行“责任·创新·贡献——CCF 2014 颁奖大会”和答谢晚宴。届时将颁发2014年度CCF终身成就奖、CCF青年科学家奖、CCF优秀博士学位论文奖、CCF杰出教育奖、CCF计算机企业家奖、CCF女计算机工作者奖、CCF卓越服务奖和CCF杰出贡献奖。此外,将通过展板和实物向来宾展示有关信息。

一种适用于云计算环境的改进全同态加密方案

作者：[锡晓峰](#)，[曹宝香](#)，[XI Xiao-feng](#)，[CAO Bao-xiang](#)
作者单位：[曲阜师范大学 计算机科学学院, 山东 日照, 276826](#)
刊名：[计算机技术与发展](#)[ISTIC](#)
英文刊名：[Computer Technology and Development](#)
年，卷(期)：2015 (2)

引用本文格式：[锡晓峰](#), [曹宝香](#), [XI Xiao-feng](#), [CAO Bao-xiang](#) 一种适用于云计算环境的改进全同态加密方案[期刊论文]-[计算机技术与发展](#) 2015 (2)