·云计算专题·　　文章编号：1000-3428(2018)08-0024-06　　文献标志码：A　　中图分类号：TP391.9

基于洋葱加密模型的同态云平台设计

李子臣[1,2,3]，杨　薇[2]，杨亚涛[2,3]，孙亚飞[2,3]，梁　斓[2,3]

（1. 北京印刷学院 信息工程学院，北京 102600；2. 北京电子科技学院 研究生系，北京 100070；
3. 西安电子科技大学 通信工程学院，西安 710071）

摘　要：在云平台服务端数据解密过程中，容易出现信息泄露、数据库管理员窥探用户隐私信息以及客户端处理任务过重等问题。为此，提出一种基于同态密码的安全云平台设计方案。在满足银行业务处理需求的私有云平台应用场景下，采用可调整洋葱加密策略，利用 Paillier 加法同态特性和 ElGamal 乘法同态特性直接操作密文，避免客户端与服务端频繁的交互及加解密处理。仿真实验与效率分析结果表明，该方案在保证运算效率的同时，可有效抵御选择明文攻击。

关键词：同态运算；洋葱加密模型；密文数据库；同态加密；私有云

中文引用格式：李子臣，杨　薇，杨亚涛，等. 基于洋葱加密模型的同态云平台设计[J]. 计算机工程，2018，44(8)：24-29.
英文引用格式：LI Zichen，YANG Wei，YANG Yatao，et al. Design of homomorphic cloud platform based on onion encryption model[J]. Computer Engineering，2018，44(8)：24-29.

Design of Homomorphic Cloud Platform Based on Onion Encryption Model

LI Zichen[1,2,3]，YANG Wei[2]，YANG Yatao[2,3]，SUN Yafei[2,3]，LIANG Lan[2,3]

（1. College of Information Engineering，Beijing Institute of Graphic Communication，Beijing 102600，China；
2. Department of Graduate Students，Beijing Electronic Science and Technology Institute，Beijing 100070，China；
3. College of Communication Engineering，Xidian University，Xi'an 710071，China）

【Abstract】 In data decryption process of cloud platform server，it is easy to cause problems of information disclosure，the database administrators spy on users' privacy information and heavy processing tasks of client. To solve above problems，a design scheme of security private cloud platform based on homomorphic cryptography is proposed. In the private cloud platform scene meeting the demand of bank business processing，by adopting with adjustable onion encryption strategy，ciphertexts can be evaluated directly by additive homomorphism of Paillier and multiplicative homomorphism of ElGamal. Then，frequent interactions between client and server，as well as data encryption and decryption operations can be avoided. Simulation experiment and efficiency analysis results show that the proposed scheme can effectively resist the chosen plaintext attack while ensuring the operation efficiency.

【Key words】 homomorphic operation；onion encryption model；ciphertext database；homomorphic encryption；private cloud
DOI：10.19678/j.issn.1000-3428.0047251

0　概述

随着云计算的发展，基于海量数据的云计算服务逐渐成为众多企业关注的重点。采用云计算处理模式开展业务十分便利，但云应用存在的安全问题也日渐凸显[1-2]，例如第三方服务提供商不可信，管理员窥探、窃取数据，造成重要信息泄露、云端资料外泄，以及数据传输过程中存在的安全隐患。将解密数据的私钥提供给服务端用于数据加解密及运算处理，可以提高系统效率，但却面临更多的安全威胁，一旦云端数据库[3]被攻陷，后果不堪设想。因此，只有用户或合法授权用户才能拥有解密数据的私钥，以确保数据安全。但该方式云端服务器只作为存储容器，无法进行有效的数据处理。数据传输及处理需要占用大量的带宽及客户端开销，无法有效利用云端的数据处理能力。

同态密码体制近乎为云计算量身打造，可以直接操作密文数据，取得与操作明文相同的效果[4]，在数据托管环境下可以确保信息的保密性，防止隐私信息泄露。文献[4]分析了同态加密技术[5]的

基金项目：国家自然科学基金(61370188)；"十三五"国家密码发展基金(MMJJ20170110)。
作者简介：李子臣(1965—)，男，教授、博士，主研方向为云计算、密码学；杨　薇(通信作者)，硕士研究生；杨亚涛，副教授、博士；孙亚飞、梁　斓，硕士研究生。
收稿日期：2017-05-18　　**修回日期：**2017-09-01　　**E-mail：**1599131213@qq.com

研究现状及在云计算环境下的应用[6]。文献[7]探讨了同态加密技术在金融云安全方面的应用,但是并没有给出具体的应用及设计方案。文献[8]提出一种同态加密在私有云中的设计方案,但未给出详细的数据存储及处理模式。文献[9-10]探索部分同态、全同态加密在密文数据库查询中的应用,其设计思想具有较高的参考价值。文献[11]提出的全同态加密方案虽然相对原始基于理想格算法复杂度有所降低,但距离实用仍有一定差距。文献[12]针对基于稀疏子集和问题的全同态加密方案提出了一种有效的反馈攻击方法,表明其存在安全隐患。

针对上述问题,本文基于文献[13]中的混合同态加密思想及文献[14]提出的洋葱加密方案,设计一种基于洋葱加密模式的同态云平台方案,以有效防止管理员窥探数据,并且使云端服务器可直接对密文进行操作而不会暴露明文状态,避免客户端与服务端的频繁交互,降低带宽需求,实现数据安全存储及运算。

1　预备知识

1.1　同态特性

令 E 为加密函数,D 为解密函数,$\oplus$表示同态加运算,$\otimes$表示同态乘运算,x 和 y 表示明文,用如下关系定义同态特性:

1)加法同态:如果存在有效算法 $\oplus$,使得 $E(x+y)=E(x)\oplus E(y)$ 或 $x+y=D(E(x)\oplus E(y))$ 成立,并且不泄漏 x 和 y,则称其具有加法同态性质。

2)乘法同态:如果存在有效算法 $\otimes$,使得 $E(x\times y)=E(x)\otimes E(y)$ 或 $xy=D(E(x)\otimes E(y))$ 成立,并且不泄漏 x 和 y,则称其具有乘法同态性质。

3)混合乘法同态:如果存在有效算法,使得 $E(x\times y)=E(x)y$ 或 $xy=D(E(x)y)$ 成立,并且不泄漏 x,则称其具有混合乘法同态性质。

4)部分同态加密(SWHE):支持有限同态加密操作的特性[15],如只支持加法同态或乘法同态运算。

1.2　Paillier 与 ElGamal 的同态性

1.2.1　Paillier 公钥密码体制同态性分析

初始化阶段:$n=pq$,其中 p、q 为 2 个大素数,定义 $\lambda=lcm(p-1,q-1)$(lcm 为最小公倍数),选择随机数 $g\in\mathbb{Z}_{n^2}^*$,需要保证 $\mu=(L(g^\lambda \bmod n^2))^{-1}$ 存在,使得 $gcd(L(g^\lambda \bmod n^2),n)=1$($gcd$ 为最大公约数),其中函数 L 定义为 $L(u)=\frac{u-1}{n}$,公钥为 (n,g),私钥为 (λ,μ)。

加密阶段:设有明文 $m\in\mathbb{Z}_n$,且 $m<n$,选择一个随机数 $r<n$,则密文为 $E(m)=g^m\cdot r^n \bmod n^2$。

解密阶段:密文 $c<n^2$,明文 $m=D[E(m)]=\frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$。

Paillier 的同态性验证过程如下:

1)对明文 x 用 Paillier 加密算法加密处理:

$E(x)=(g^x\cdot r_1^n) \bmod n^2$

2)对明文 y 用 Paillier 加密算法加密处理:

$E(y)=(g^y\cdot r_2^n) \bmod n^2$

3)对明文 x 和明文 y 对应密文进行乘积运算:

$$E(x)\oplus E(y)=(g^x\cdot r_1^n)\oplus(g^y\cdot r_2^n) \bmod n^2=(g^{x+y}\cdot(r_1r_2)^n) \bmod n^2=E(x+y)$$

由上述推理过程可知,对明文 x 和 y 对应的密文进行乘积运算,所得结果与明文 x 和 y 加和后对应的密文值相同。由此得证,Paillier 公钥密码体制具有加法同态特性。

1.2.2　ElGamal 公钥密码体制同态性分析

初始化阶段:选取大素数 p,g($g<p$)是循环群 $\mathbb{Z}_p^*$ 的生成元,在循环群中选取随机数 x 作为私钥,公钥参数 $y=g^x \bmod p$,公钥(y,g,p)。

加密阶段:选取与($p-1$)互素的随机数 k,$E(m)=(a,b)=(g^k \bmod p,\ y^k m \bmod p)$。

解密阶段:$m=D[E(m)]=D(a,b)=b\cdot a^{-x}$。

ElGamal 的同态性验证过程如下:

1)对明文 m_1 用 ElGamal 加密算法加密处理:

$E(m_1)=(a_1,b_1)=(g^{k_1} \bmod p,\ y^{k_1}m_1 \bmod p)$

2)对明文 m_2 用 ElGamal 加密算法加密处理:

$E(m_2)=(a_2,b_2)=(g^{k_2} \bmod p,\ y^{k_2}m_2 \bmod p)$

3)对明文 x 和明文 y 对应密文进行乘积运算:

$$E(m_1)\otimes E(m_2)=(a_1a_2,b_1b_2)=(g^{k_1+k_2} \bmod p,\ y^{k_1+k_2}(m_1\cdot m_2) \bmod p)=E(m_1\cdot m_2)$$

由上述推理过程可知,对明文 m_1 和 m_2 对应的密文进行乘积运算,所得结果与明文 m_1 和 m_2 相乘后对应的密文值相同。由此得证,ElGamal 公钥密码体制具有乘法同态特性。

2　方案设计

2.1　银行私有云平台整体架构

本文旨在应用同态加密技术解决云端数据安全存储及处理等问题,探索同态加密在私有云平台应用场景下的应用方式,在此对私有云平台具体功能模块不作详细说明。银行私有云平台整体架构如图 1所示。

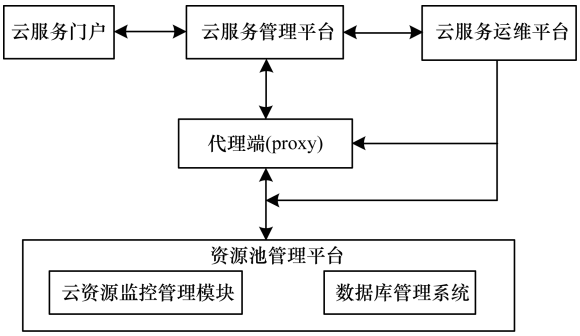


图 1 银行私有云平台系统架构

云服务门户:接收用户查询、处理请求,以可视化方式进行内容发布和更新、参数管理,并提供外部系统的接口。

云服务管理平台:支持对系统提供服务的管理功能,根据银行业务处理需求确定功能模块。

云服务运维平台:分析监控数据,向监控平台提供监控数据和配置数据,以确保整个运维体系的完备性。

代理端(proxy):是本文设计方案的重要模块,用于拦截应用程序端发送的查询、处理请求,对查询语句、请求参数进行重写,并发送可执行的 SQL 操作语句和密文参数给数据库管理系统(Database Management System,DBMS),与 DBMS 联合完成对密文的查询处理。

资源池管理平台:将计算、网络、存储等资源进行统一化、标准化并抽象为原子服务。

2.2 系统交互流程

本文方案中银行私有云安全系统由两部分组成,一部分为客户端(A),另一部分为云平台,即处理和存储密文数据的服务端(B)。客户端拥有 Paillier 加解密的公钥(n,g)和私钥(p,q),以及 ElGamal 加解密的公钥(y,g,p)和私钥 x。服务器端已知客户端公钥,无解密数据的私钥,无法解密密文数据,确保了信息的安全性。

根据方案设计,银行私有云平台客户端 A 与服务器端 B 的数据交互过程如图 2 所示。

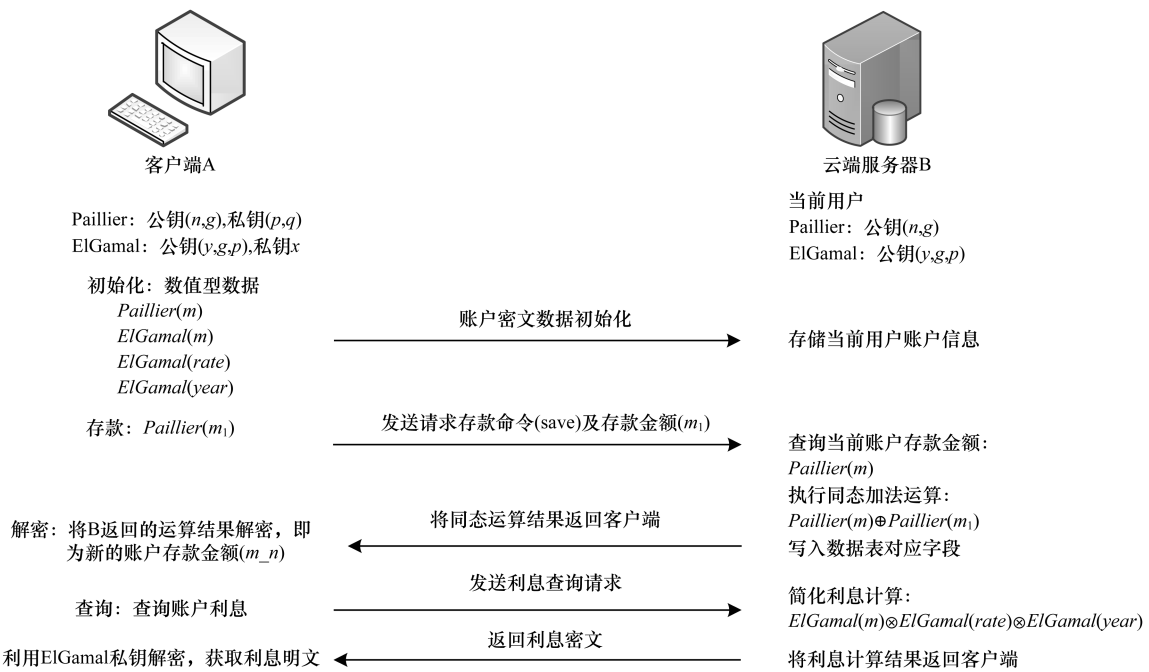


图 2 银行私有云平台客户端 A 与服务器端 B 的数据交互过程

下面以银行账户存款、利息查询操作为例,描述客户端 A 和服务端 B 的数据交互过程。

1)数据初始化。客户端拥有 Paillier 和 ElGamal 加解密算法的公私钥对。对数值型数据初始化洋葱层,使用 Paillier 算法加密数据形成 oADD 洋葱,支持密文加运算;使用 ElGamal 算法加密数据形成 oMUL 洋葱层,支持乘法运算。

2)存款。客户端根据用户命令,选取 Paillier 算法加密存款金额,发送存款请求命令到服务端。

3)服务端根据客户端请求,对原始账户 Paillier 加密密文与接收的存款密文执行加法同态运算,将运算结果写入数据表并返回给客户端;客户端对返回结果使用 Paillier 私钥解密,此时的明文即为存款后最新账户金额 m_n。

4)客户端发送利息查询请求到服务端;服务端根据客户端查询命令,利用 oMUL 洋葱的乘法同态特性完成利息运算:$ElGamal(m)\otimes ElGamal(rate)\otimes ElGamal(year)$。

5)服务端将运算结果返回给客户端,由客户端使用 ElGamal 私钥进行解密,获取利息明文。

2.3　数据存储结构

本文方案对数据的处理采用多洋葱分层加密方式,根据操作目的的不同,设计了 EQ、ORD、SEARCH、oADD、oMUL 5 种洋葱。

1)EQ 洋葱用于等值匹配查询,由 3 个洋葱层组成:最外层洋葱(RND)采用概率加密算法提供最强的安全性,不用于支持密文操作;中间洋葱层(DET)采用确定性加密算法,支持密文等值查询功能,但安全性相对 RND 略弱;最内层洋葱层(JOIN)提供不同字段列的连接操作功能。

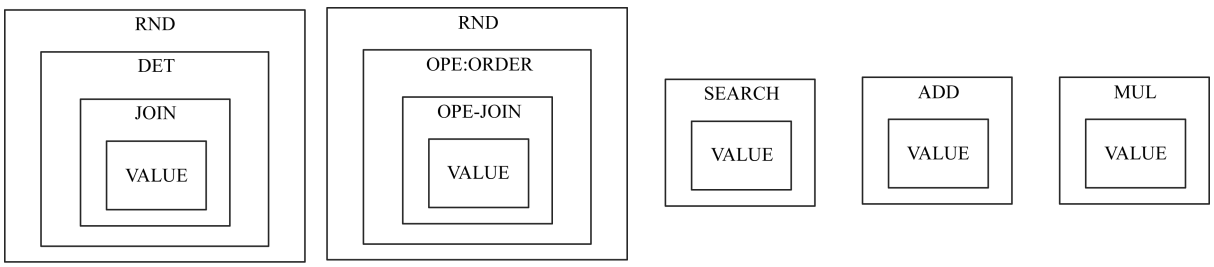
2)ORD 洋葱支持对密文数据大小关系的比较,由 3 个洋葱层组成:最外层、最内层与 EQ 洋葱功能近似;中间洋葱层采用保序对称加密算法加密,使得密文与明文具有相同的大小偏序关系,可以支持数据库基础 ORDER BY、MIN、MAX 等函数功能实现。

3)SEARCH 洋葱支持加密文本信息的关键字检索,采用文献[16]提出的可搜索加密方案实现,检索过程无需解密数据,可确保信息的机密性。

4)oADD 洋葱支持数值型数据的加法和减法同态运算,为单洋葱层结构,采用具有加法同态特性的密码算法加密实现,如 Paillier 加密算法。

5)oMUL 洋葱支持数值型数据的乘法同态运算,为单洋葱层结构,采用具有乘法同态特性的密码算法实现,如 RSA/ElGamal 加密算法。

洋葱的安全性等同于最外层洋葱的安全性。一旦数据库表创建,所有洋葱都处于最安全的层次。5 种洋葱的层次结构如图 3 所示。



(a)EQ 洋葱　(b)ORD 洋葱　(c)SEARCH 洋葱　(d)oADD 洋葱　(e)oMUL洋葱

图 3　本文方案的洋葱层次结构

鉴于篇幅原因,前 3 种洋葱在此不作详细论述,本文主要针对 oADD、oMUL 洋葱实现数值型数据的同态操作进行阐述。在银行私有云平台应用场景下,简化的存储表结构如图 4 所示。其中,ID 表示银行账户编号,NAME 表示账户名,ACCOUNT 表示账户金额。经过洋葱加密,云端数据表中存储方式如图5所示。其中,C1-EQ、C1-ORD、C1-oADD、C1-oMUL 表示分别采用等值洋葱、保序洋葱、同态洋葱进行加密。

Account_t		
ID	NAME	ACCOUNT

图 4　数据库账户存储简化表结构

Account_t													
C1-IV	C1-EQ	C1-ORD	C1-oADD	C1-oMUL	C2-IV	C2-EQ	C2-ORD	C2-SEARCH	C3-IV	C3-EQ	C3-ORD	C3-oADD	C3-oMUL

图 5　云端数据存储方式

同态洋葱是本文方案的重点设计模块。对于数值型数据,通常执行等值匹配、大小比较、加减乘除等运算,系统会根据数据类型创建并初始化洋葱。根据用户操作需求调整到特定的洋葱层。以用户的存款请求为例,需要对当前账户金额执行加运算,服务端根据用户的加操作请求查找 ACCOUNT 字段对应的 oADD 洋葱,获取当前层的密文数据。

在处理用户请求过程中,代理端对存款金额进行查询重写,以存款金额 m_1 为例,代理端采用 Paillier 算法加密 m_1 生成对应的密文 m_1',服务端执行如下命令完成数据更新:

```
update Account_t set C3-oADD =
        ACCOUNT_ADD(key,C3-IV,C3-oADD + m1');
```

对当前 C3-oADD 字段值与使用 Paillier 密码体制进行加密的存款值执行同态加运算,并将该值存储到数据库中指定字段。将新的运算结果返回客户端,由用户使用私钥解密,终端会显示新的账户存款金额。用户请求查询账户利息,服务端查找账户金额对应的 oMUL 洋葱,对当前值与银行利率、存款期

限执行同态乘运算,并将运算结果返回客户端进行解密,显示账户利息金额。

3 方案分析

3.1 计算深度控制分析

Paillier 与 ElGamal 公钥密码体制同态操作的深度与模数相关,当数据超过模数值时,会存在数据重叠出错,使数据无法正常解密。本文方案在加解密过程中,在每次密文操作后进行取模处理,以降低密文的规模,实现密文噪声控制。

3.2 浮点数映射过程分析

银行数据库中除了用户身份等文本信息,还包括大量的数值型数据,涉及浮点型数据、大整数等,这就需要系统具有浮点数及大数处理能力。银行账户金额、利率等数值通常为浮点数,因此,将浮点数映射为整数进行处理,最后通过逆映射还原数据。对于大数处理采用 NTL 库实现,可以对任意位数的数据进行处理。映射方式如下:

1)$y=\alpha_0.\alpha_1\alpha_2\cdots\alpha_k$,$y$ 为浮点数,其中,α_0 表示整数部分,$\alpha_1\alpha_2\cdots\alpha_k$ 表示小数点后 k 位。根据小数点后数值位数 k 进行映射处理。

2)将浮点数放大 k 倍映射为 $y'=\alpha_0\times10^0+\alpha_1\times10^1+\alpha_2\times10^2+\cdots+\alpha_k\times10^k$。浮点数存储时可以表示为$(y',k)$。

3)逆映射可以表示为 $a_i=f^{-1}(y')=\dfrac{y'}{10^i}$,还原浮点数 $y=\alpha_0.\alpha_1\alpha_2\cdots\alpha_k$。

3.3 安全性与效率分析

本文方案基于 Paillier 和 ElGamal 公钥密码体制的加法和乘法同态特性进行数据运算,在服务器端存储密文数据,客户端拥有解密密文的密钥。客户端向服务器端发送数据处理请求,服务器端没有解密私钥,只能操作密文数据,无法解密密文,从而确保服务端管理员无法窥探用户隐私信息,即使数据库被攻陷也不会造成隐私信息泄露。

文献[7]中用 RSA 同态特性实现乘法运算的方案,其安全性依赖于大数分解,且密钥产生受素数产生限制,难以做到一次一密。而 ElGamal 算法安全性依赖于计算有限域上离散对数这一难题。相较于 RSA,ElGamal 体制随机参数的选取每次均不同,即使使用相同的私钥对相同明文进行加密,得到的密文值也各不相同,使密文不仅依赖于明文,而且依赖于选取的随机数,相同的明文对应不同的密文,可抵御选择明文攻击,具有更高的安全性。

本文方案是在银行私有云平台的应用场景下,利用 Paillier 和 ElGamal 密码体制的加法和乘法同态特性实现,在服务端直接对密文执行运算,基本可以满足银行对账户数值型数据的处理需求。服务器端只需执行简单的同态操作,降低了数据处理复杂性。

文献[7]设计了基于 RSA 和 Paillier 同态特性的云计算方案,并与文献[17]提出的 DGHV 全同态加密方案进行对比分析。为论证本文方案的效率,对 3 种方案进行仿真实现,并进行效率及安全性对比。以对10^4 大小的整数进行加解密处理为例,ElGamal、RSA 密钥长度均为 1 024 bit,由于操作环境的局限,在此简化仿真过程,在同一台 PC 机上对方案同态运算进行仿真实现和效率分析。3 种方案的平均运算时间与安全性分析如表 1 所示。

表 1 3 种方案的同态运算时间及安全性比较

方案	平均运算时间/ms	安全性
本文方案	377	选择明文安全
文献[7]方案	327	无法抵御选择明文攻击
文献[17]方案	23 891	选择明文安全

由表 1 可知,对于同等长度的密钥,本文方案相比文献[7]方案运算效率略有降低,但效率明显高于文献[17]的全同态加密方案。相对于在服务器端解密数据完成操作,应用同态特性运算速率略有降低,但是具有更高的安全性,可防止明文信息被窃取。此外,采用同态加解密方式,可以在服务端直接操作密文,避免频繁将数据传回客户端进行解密,使交互双方通信次数减少一半,降低了带宽压力及数据传输过程中的安全风险。

4 结束语

本文提出一种基于洋葱加密模型的同态云平台设计方案。在银行私有云平台应用场景下,充分利用云计算能力,基于密码体制的同态特性,结合可调整洋葱加密策略,从而降低客户端数据处理开销,提高系统的安全性和可靠性,并提供一种可用于数据存储和管理的可扩展结构。仿真及安全性分析结果表明,本文方案在保证运算效率的情况下,具有较高的安全性,可有效抵御选择明文攻击,满足银行业务处理需求。下一步将对该方案占用存储空间略有增加的问题进行优化。

参考文献

[1] 俞能海,郝　卓,徐甲甲,等. 云安全研究进展综述[J]. 电子学报,2013,41(2):371-381.

[2] GHORBEL A, GHORBEL M, JMAIEL M. Privacy in cloud computing environments: a survey and research challenges [J]. Journal of Supercomputing, 2017, 73(6):2763-2800.

[3] LÄNGER T, PÖHLS H C, GHERNAOUTI S. Selected cloud security patterns to improve end user security and privacy in public clouds[M]//SCHIFFNER S, SERNA J, LKONOMOU D, et al. Privacy Technologies and Policy. Berlin, Germany: Springer, 2016.

[4] 李顺东,窦家维,王道顺. 同态加密算法及其在云安全中的应用[J]. 计算机研究与发展,2015,52(6):1378-1388.

[5] HRESTAK D, PICEK S. Homomorphic encryption in the cloud [C]//Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics. Opatija, Croatia: [s. n.], 2014:1400-1404.

[6] SHAHZAD F, IQBAL W, BOKHARI F S. On the use of CryptDB for securing electronic health data in the cloud: a performance study [C]//Proceedings of the 17th International Conference on E-health Networking, Application and Services. Boston, USA: [s. n.], 2015: 120-125.

[7] TEBAA M, ZKIK K, HAJJI S E. Hybrid homomorphic encryption method for protecting the privacy of banking data in the cloud[J]. International Journal of Security and Its Applications, 2015, 9(6):61-70.

[8] 陈志伟,杜　敏,杨亚涛,等. 基于 RSA 和 Paillier 的同态云计算方案[J]. 计算机工程,2013,39(7):35-39.

[9] BONEH D, GENTRY C, HALEVI S, et al. Private database queries using somewhat homomorphic encryption [C]// Proceedings of International Conference on Applied Cryptography and Network Security. Banff, Canada: [s. n.], 2013:102-118.

[10] ZHAO F, LI C, LIU C F. A cloud computing security solution based on fully homomorphic encryption[C]// Proceedings of the 16th International Conference on Advanced Communication Technology. Pyeongchang, South Korea: [s. n.], 2014:485-488.

[11] 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.

[12] 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.

[13] KANGAVALLI R, VAGDEVI S. A mixed homomorphic encryption scheme for secure data storage in cloud[C]//Proceedings of Advance Computing Conference. Washington D.C., USA: IEEE Press, 2015:1062-1066.

[14] POPA R A, REDFIELD C M S, ZELDOVICH N, et al. CryptDB: processing queries on an encrypted database [J]. Communications of the ACM, 2012, 55(9):103-111.

[15] CARDELLINI V, IANNUCCI S. Designing a flexible and modular architecture for a private cloud [C]// Proceedings of International Workshop on Virtualization Technologies in Distributed Computing. [S. l.]: USENIX, 2012:37-44.

[16] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data [C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2002:44-55.

[17] DIJK M V, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers [M]//GILBERT H. Advances in Cryptology-EUROCRYPT 2010. Berlin, Germany: Springer, 2010:24-43.

编辑　金胡考

(上接第 23 页)

[5] 闫玺玺,汤永利. 数据外包环境下一种支持撤销的属性基加密方案[J]. 通信学报,2015,36(10):92-100.

[6] 潘　宁,朱智强,孙　磊,等. 一种用于云存储的可撤销的属性加密方案[J]. 计算机应用研究,2014,31(5):1488-1490.

[7] 方雪锋,王晓明. 可撤销用户的外包加解密 CP-ABE 方案[J]. 计算机工程,2016,42(12):124-128.

[8] 刘竹松,彭佳鹏. 一种支持属性撤销的外包属性加密方案[J]. 计算机工程,2017,43(10):109-114.

[9] CHASE M. Multi-authority attribute based encryption[M]. Berlin, Germany: Springer, 2007:515-534.

[10] CHEN J, MA H. Efficient decentralized attribute-based access control for cloud storage with user revocation [C]// Proceedings of IEEE International Conference on Communications. Washington D.C., USA: IEEE Press, 2014: 3782-3787.

[11] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Computer Society, 2007:321-334.

[12] 李继国,石岳蓉,张亦辰. 隐私保护且支持用户撤销的属性基加密方案[J]. 计算机研究与发展,2015,52(10):2281-2292.

[13] 张亮轩,李　晖. 云计算中支持有效用户撤销的多授权方基于属性加密方案[J]. 网络与信息安全学报,2016,2(2):62-74.

[14] BEIMEL A. Secure schemes for secret sharing and key distribution[J]. International Journal of Pure & Applied Mathematics, 1996, 3(3).

[15] 杨浩淼,孙世新,李洪伟. 双线性 Diffie-Hellman 问题研究[J]. 四川大学学报(工程科学版),2006,38(2):137-140.

[16] 雷丽楠,李　勇. 基于密文策略属性基加密的多授权中心访问控制方案[J]. 计算机应用研究,2018,35(1):248-252,276.

编辑　索书志