计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2015.20131494
52(6):1378-1388,2015

同态加密算法及其在云安全中的应用

李顺东[1] 窦家维[2] 王道顺[3]
[1](陕西师范大学计算机科学学院 西安 710062)
[2](陕西师范大学数学与信息科学学院 西安 710062)
[3](清华大学计算机科学与技术系 北京 100084)
(shundong@snnu.edu.cn)

Survey on Homomorphic Encryption and Its Applications to Cloud Security

Li Shundong[1], Dou Jiawei[2], and Wang Daoshun[3]
[1](*School of Computer Science, Shaanxi Normal University, Xi'an* 710062)
[2](*School of Mathematics and Information Science, Shaanxi Normal University, Xi'an* 710062)
[3](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

Abstract Cloud service mode has great economical and technical advantages and wide application prospects. The popularization of the cloud service is significant to both the informationization and the development of China. Cloud security is the most serious challenge in the generalization and the applications of the cloud service. Homomorphic encryption schemes, especially fully ones, are the most important technology to solve the security problem arising in cloud service, and a focus in the international cryptographic community. In this paper, we summarize the state of the art of the homomorphic encryption research, introduce the applications of the homomorphic encryption to the protection of the data confidentiality in cloud computing and to other fields, analyze the merits and the faults of various algebraic somewhat homomorphic encryption schemes and of fully homomorphic encryption schemes based on circuits, point out some open problems and new directions in the fully homomorphic encryption research, and briefly introduce the concept of secure plaintext computing, its advantages over cipher-text computing and some problems that need further studying.

Key words cryptography; cloud service; homomorphic encryption; cipher-text computation; secure multiparty computation

摘 要 云服务模式具有巨大的经济技术优势和广阔的应用前景,普及云服务技术对我国的信息化建设和社会发展具有重要的意义.云服务推广与应用中面临的最大挑战是安全问题.同态加密,尤其是全同态加密是解决云服务安全问题极为关键的技术,也是近年来国际密码学界研究的热点问题.对同态加密的研究现状进行了综述,介绍了同态加密在云计算机密性保护及其他方面的应用,重点介绍了各种代数部分同态加密方案和电路全同态加密方案的优缺点.对同态加密未来的研究问题进行了分析,同时简单介绍了云安全中的明文保密计算概念、相对于密文计算的优势以及需要进一步研究的问题等.

关键词 密码学;云服务;同态加密;密文计算;多方保密计算

中图法分类号 TP393;TN918

收稿日期:2013-11-18;**修回日期**:2014-07-21

基金项目:国家自然科学基金项目(61272435,61373020,61070189)

云服务是一种新的服务交付和使用模式.在这种模式下云服务商负责购买、维护、管理和升级计算软硬件设施,并通过网络以按需、易扩展的方式向云用户提供满足需要的计算与存储服务,而用户则按照使用资源的情况支付使用费.云服务可以大大地节约数据管理、软硬件购买、系统管理维护和升级的费用,同时可以获得满足需要的存储与计算能力,因而云服务模式具有巨大的经济技术优势和广阔的应用前景[1].普及云服务技术对我国的信息化建设和社会发展具有重要的意义.

云服务给用户带来了超强的计算能力、近乎无限的存储能力和巨大的经济利益,同时也带来了严重的安全问题.云服务的实际应用面临诸多挑战,其中安全问题被认为是最大的挑战,是云服务亟待解决的最大难题[2-3].思科 CEO 钱伯斯甚至夸张地说"云计算是安全的噩梦[4]".云服务安全问题非常复杂,需要研究解决的问题很多.在诸多的安全问题中,数据的机密性保护是云服务中最重要、最关键的安全问题,这涉及到数据的保密存储与保密计算,是云存储和云计算中最关键的安全问题.

首先,机密数据采用云存储会造成巨大的安全隐患[5].如果用户把机密信息以明文形式存储在云服务商处,云服务商就可以复制机密信息为自己谋利且不影响云服务商给用户提供完整的信息,用户根本无法发现自己的信息已被复制或泄露,但机密信息的价值就会大打折扣甚至完全丧失,若被敌方利用还可能造成致命的损失.因此,在云存储中如何面对云服务商保持数据的机密性是云用户最关心的安全问题.从理论上讲,同态加密存储是一种可行的解决方案.其次,云用户若将原本由自己完成的计算任务外包给云去完成,如果是机密数据,这样做就会导致机密数据泄露.即使是加密的数据,要利用云完成计算也必须首先解密,同样会泄露给云服务商.明文保密计算是这个问题的可能解决方案.同态加密与云服务中数据机密性保护密切相关,是解决云服务数据机密性保护问题的关键技术,也是密文检索的关键技术.解决云服务机密性保护问题的迫切需要推动了同态加密研究的繁荣,同态加密技术的突破将使云服务关键安全问题获得满意的解决.

本文总结了云服务中数据机密性保护的关键技术——同态加密技术的研究现状、不足、需要进一步研究的问题和各种可能的应用;主要介绍了各种代数部分同态加密算法和电路全同态加密算法的优缺点;同时简单介绍了明文保密计算的概念、明文保密计算在数据机密性保护方面的作用、相对于密文计算的优势以及需要进一步研究的问题.

1 预备知识

1.1 部分同态加密

同态是近世代数中的概念.设$\langle G,*\rangle$和$\langle H,\circ\rangle$是 2 个代数系统,$f:G\to H$是一个映射,如果对于$\forall a,b\in G$,都有$f(a*b)=f(a)\circ f(b)$,则称f是从G到H的一个同态映射.密码学推广了近世代数的同态映射概念,提出了部分同态与全同态加密概念.Rivest,Adleman 和 Dertouzos[6]首先发现 RSA 公钥加密算法[7]具有部分同态性,受此启发他们提出了同态加密的概念[6].Rappe[8]探讨了同态加密的各种应用.加密是从明文空间到密文空间的映射,如果加密映射是一个同态映射,我们就说它是一个同态加密方案.简单地说同态加密就是加密运算和某一代数运算或者混合代数运算可以交换顺序的加密方案.目前尚没有简洁的、普遍接受的同态加密定义,笔者根据自己对同态加密的理解,给出如下定义:

定义 1. 设$E(K,x)$表示用加密算法E和密钥K对x进行加密,F表示一种运算,如果对于加密算法E和运算F,存在有效算法G使得:

$$E(K,F(x_1,\cdots,x_n))=G(K,F,(E(x_1),\cdots,E(x_n))),\tag{1}$$

就称加密算法E对于运算F是同态的.

如果定义中的等式仅对$F(x_1,\cdots,x_n)=\sum_{i=1}^{n}x_i$成立,那么该加密方案就是一个加法同态加密方案(additively homomorphic encryption).

如果定义中的等式仅对$F(x_1,\cdots,x_n)=\prod_{i=1}^{n}x_i$成立,那么该加密方案就是一个乘法同态加密方案(multiplicatively homomorphic encryption).

如果定义中的等式对包含加法与乘法混合运算的$F(x_1,\cdots,x_n)$成立,那么该加密方案就是一个全同态加密方案(fully homomorphic encryption).只对一种运算成立的同态加密方案称为部分同态加密方案(somewhat homomorphic encryption or partially homomorphic encryption).理解了这个定义,就可以很自然地理解同态加密各种应用.

ElGamal 乘法同态加密算法[9]:设p是一个大素数,g是Z_p^*的一个生成元,任意选择一个随机数$k\in Z_p^*$作为私钥,计算$h=g^k \bmod p$,将其作为公钥.

要加密消息 $m<p$,任意选择一个随机数 $r\in Z_p^*$,计算:

$$c_1 = g^r \bmod p, c_2 = mh^r \bmod p.$$

m 的密文就是 $E(m)=(c_1,c_2)=(g^r,mh^r)$. 因为

$$E(m_1)E(m_2) = (g^{r_1},m_1h^{r_1})(g^{r_2},m_2h^{r_2}) = (g^{r_1+r_2},m_1m_2h^{r_1+r_2}) = E(m_1+m_2),$$

所以 ElGamal 公钥加密算法具有乘法同态性.

Paillier 加法同态加密算法[10]:设 p,q 为大素数,$n=pq$. $\lambda=lcm(p-1,q-1)$,定义

$$L(u) = \frac{u-1}{n}.$$

假设 g 满足:

$$gcd((g^\lambda \bmod n^2),n) = 1,$$

要加密消息 $m<n$,选择一个随机数 $r<n$,则密文为

$$E(m) = g^m r^n \bmod n^2.$$

因为

$$E(m_1)E(m_2) = (g^{m_1}r_1^n)(g^{m_2}r_2^n) = g^{m_1+m_2}(r_1r_2)^n = E(m_1+m_2 \bmod n),$$

所以 Paillier 公钥加密算法具有加法同态性.

部分同态加密方案的构造没有规律可循,主要是利用数论和近世代数中某些代数运算的性质结合某些计算困难问题构造具有部分同态性的公钥加密方案,构造的方法见仁见智. ElGamal 和 Paillier 公钥加密算法是 2 个典型的部分同态加密算法,此外著名的 RSA 公钥加密算法[6]也具有乘法同态性,Benaloh 加密算法[11]具有加法同态性,Goldwasser-Micali 加密算法[12]具有异或同态性.

1.2 全同态加密

式(1)给出的全同态加密算法的定义非常简洁,但到目前为止人们还没有找到利用这种定义构造的全同态加密方案. 实际的全同态加密方案主要是利用电路构造的,所以全同态加密方案也是用电路来定义的. 电路计算是计算理论中一种重要的计算模型[13],只有理解了电路计算,才能理解全同态加密方案的定义. 如果不理解电路计算模型,可以将其看成一个函数来理解. 由于"一个电路理论上等价于一个函数",所以对于电路 C,当出现 $C(x_1,\cdots,x_n)$ 时,可以认为它等价于某个函数 $F(x_1,\cdots,x_n)$. 本文采用文献[14]对于全同态加密方案的定义.

一个常规的(conventional)公钥加密方案 ε 由 $KeyGen_\varepsilon$, $Encrypt_\varepsilon$ 和 $Decrypt_\varepsilon$ 这 3 个随机算法组成. $KeyGen_\varepsilon$ 接收安全参数 λ 作为输入,输出私钥 sk 与公钥 pk, pk 定义了明文空间 P 和密文空间 X. $Encrypt_\varepsilon$ 接收输入 pk 和明文 $\pi\in P$,输出用公钥 pk 加密明文 π 所得的密文 $\psi\in X$,记作 $\psi=Encrypt_\varepsilon(pk,\pi)$. $Decrypt_\varepsilon$ 接收输入 sk 和 ψ,输出明文 π. 上述 3 个随机算法的计算复杂性都应该是 λ 的多项式. 加密系统还应满足正确性条件:即如果 $(sk,pk)\xleftarrow{R}KeyGen_\varepsilon(\lambda)$,而且 $\pi\in P$, $\psi\xleftarrow{R}Encrypt_\varepsilon(pk,\pi)$,那么 $Decrypt_\varepsilon(sk,\psi)=\pi$.

同态加密方案除了上述 3 个随机算法外,还有一个算法 $Evaluate_\varepsilon$:输入公钥 pk、从电路集合 C_ε 中选取的一个电路 C 以及一组密文 $Y=\langle\psi_1,\cdots,\psi_t\rangle$,输出密文 $\psi\in C$. 如果:

$$\psi_i = Encrypt_\varepsilon(pk,\pi_i),\ i=1,\cdots,t,$$

那么

$$Evaluate_\varepsilon(pk,Y,C) = Encrypt_\varepsilon(pk,C(\pi_1,\cdots,\pi_t)). \quad (2)$$

定义 2[14]. 如果同态加密方案 ε 对于 $KeyGen_\varepsilon(\lambda)$ 生成的任何密钥对 (sk,pk),任意电路 $C\in C_\varepsilon$,任意密文 $Y=\langle\psi_1,\cdots,\psi_t\rangle$,其中 $\psi_i=Encrypt_\varepsilon(pk,\pi_i)$,如果 $\psi=Evaluate_\varepsilon(pk,Y,C)$ 则 $Decrypt_\varepsilon(sk,\psi)=C(\pi_1,\cdots,\pi_t)$,就说同态加密方案 ε 对于电路集合 C_ε 是正确的.

定义 3[14]. 如果存在一个多项式 f,对于任意的安全参数值 λ,同态加密方案 ε 的解密算法可以用一个规模(size)最多为 $f(\lambda)$ 的电路 D_ε 表示,就说同态加密方案 ε 是紧凑的(compact).

定义 4[14]. 如果加密方案 ε 对于 C_ε 中的电路是紧凑且正确的,就说同态加密方案 ε 紧凑地计算 C_ε 中的电路.

定义 5[14]. 如果一个同态加密方案 ε 能够紧凑地计算所有电路,就说它是全同态的.

这里给出的同态加密定义很难理解,也很难在这样的定义基础上理解同态加密的各种应用. 基于电路计算模型的全同态加密方案定义已经很复杂了,基于电路计算模型的全同态加密算法的构造更为复杂,一般是先构造一个能够用电路表示的部分同态加密方案,然后修改电路使这个电路成为自举电路(bootstrapable circuit),从而成为全同态加密电路. 全同态加密方案的构造过程很难用较短的篇幅完整地描述.

1.3 同态加密与云安全

在利用云服务的过程中要保证数据的机密性应该分别考虑下面 2 种情况:1)参与计算的数据是加密存储的;2)参与计算的机密数据是用户自己以明文方式保存的.

如果参与云计算的数据是以加密形式存储的,人们自然希望直接利用加密的数据进行计算.如果能够直接利用密文进行计算,那么即使云参与了计算过程,仍可保证数据的机密性.目前只有利用同态加密才能够实现在密文上直接计算.理论上讲,如果采用全同态加密算法对数据进行加密存储,用户就可以利用云在多个密文上直接进行任何运算,运算的结果等于对相应的多个明文进行直接运算所得结果的密文,即

$$G(K,F,(E(x_1),\cdots,E(x_n)))=E(K,F(x_1,\cdots,x_n)),$$

故用户可以将 $x_1,\cdots,x_n$ 加密成密文 $E(x_1),\cdots,E(x_n)$存储在云中,这就可以防止云服务商对数据的无授权访问.需要借助云计算 $F(x_1,\cdots,x_n)$时,让云直接在密文上计算 $G(K,F,(E(x_1),\cdots,E(x_n)))$,得到结果后再进行解密就可以得到 $F(x_1,\cdots,x_n)$,从而实现保密计算 $F(x_1,\cdots,x_n)$,而且避免了重复加密解密,这种计算称为密文计算(cipher-text computation).这意味着用户可以在不信任云服务商的条件下,利用云进行保密存储与保密计算,这同时解决了云服务的保密存储与保密计算问题.因此,同态加密成为云计算与云存储中保证数据机密性的核心技术,也是多用户联合保密计算,即多方保密计算[15-18]的重要技术.

如果参与计算的机密数据是用户以明文形式保存的,这种情况对应于明文保密计算,目前对这种情况研究的很少,但要实现机密数据的计算外包就必须解决这种情况下特殊的安全问题.关于明文保密计算的内容,将在 2.4 节介绍.

2 同态加密的研究现状

2.1 部分同态加密算法

RSA 算法是建立在因子分解困难性假设基础上的公钥加密算法,使用电子密码本模式(electronic code book)进行加密时,RSA 加密算法具有乘法同态性,乘法同态性表现为 $E(m_1)E(m_2)=E(m_1m_2)$,这对应于定义 1 中 F,G 都是乘法运算的情况.RSA 是第一个具有部分同态性的加密算法.

自 RSA 公钥加密算法之后,人们又相继构造了多种具有部分同态性的加密算法.其中,建立在计算有限域上离散对数困难性假设基础上的 ElGamal 算法[9]具有乘法同态性,它是一个概率公钥加密算法,既能用于加密又能用于数字签名;Cramer[19]提出了具有加法同态性的变形 ElGamal 算法,但是这个算法的解密过程需要计算离散对数,而计算离散对数是困难的;建立在计算以合数为模的二次剩余困难性假设基础上的 Goldwasser-Micali 概率加密算法[12]具有对异或运算的同态性,这种同态性表现为 $E(m_1)\oplus E(m_2)=E(m_1\oplus m_2)$,该算法对数据的加密只能逐比特进行;建立在理想成员资格判定问题(ideal membership problem)基础上的 Benaloh 算法[11]对于 Z_n 上的加法运算具有同态性;建立在合数模的高阶剩余计算困难性假设基础上的 Paillier 算法[10]具有加法同态性,这种同态性表现为 $E(m_1)E(m_2)=E(m_1+m_2 \bmod n)$,这对应于定义中 F 为加法运算、G 为乘法的情况;Naccache-Stern 算法[20]是基于高阶剩余计算困难性假设的公钥密码算法,具有乘法同态性;基于因子分解困难性假设的 Okamoto-Uchiyama 算法[21]和基于不经意传输方法构造的 Damgard-Jurik 算法[22]也具有加法同态性.同态加密算法有确定性同态加密算法和概率同态加密算法,Dam,Hallgren 和 Ip[23]证明了在量子计算环境中任何确定性同态加密算法都可以在多项式时间内被攻破,不具有语义上的安全性(semantic security).上述算法中只有 RSA 算法是确定性算法,其他算法都是概率加密算法.概率同态加密算法每加密一个分组就需要选择一个随机数,对于同一个分组每一次加密的结果都不相同,因此这些概率同态加密算法都是语义安全的.

2.2 全同态加密算法

部分同态加密算法虽然有许多重要应用,但其应用范围仍然很有限,要解决云服务中的关键安全问题必须借助于全同态加密算法,因此构造全同态加密算法成为密码学界一个重要的公开问题(central open problem).人们在寻求构造全同态加密算法的过程中,构造了同时对加法和乘法同态的 Boneh-Goh-Nissim(BGN)加密算法[24].BGN 同态加密算法是利用代数环的结构特性构造的,可以进行任意次数的加法同态运算,但只能做一次乘法同态运算,它可以用于计算二阶析取范式公式的同态加密(homomorphic evaluation of 2-DNF formulas).BGN 之后又诞生了可以计算密文的任何电路的同态加密算法[25],但密文的长度是电路深度的指数函数.因为理论上电路与函数可以互相转化,所以只要能计算密文的任何电路就可以进行任意的同态加密.

上述2种全同态加密算法[24-25]的安全性都是基于理想成员问题(ideal membership problem)假设,称为传统(conventional)同态加密算法.对于加法和乘法同态的算法还有基于格(lattice)上的唯一最短向量问题(unique shortest vector problem)到最坏情况的归约问题的链式加密方案(chained encryption scheme)[26]和基于RS线性码(Reed-Solomon-code-based)的方案[27],它们的密文长度也是随电路深度指数增加的,而且密文中蕴含错误信息,经过一次加密的密文在解密时可以消除错误信息而正确解密.进行多次同态运算时,错误信息也随着增加,如果运算的次数较多,错误可能积累到无法正确解密的程度.在探索高效的同态加密方案方面,Gentry在文献[14]中提到Dijk[28]提出了一种对称的同态加密方案,但该方案一次只能加密1 b,而且对于格归约攻击是不安全的[14].文献[29-30]用部分同态加密算法构造了NC1电路(一类深度为$O(\log n)$、电路门数为多项式、扇入数为常数的电路)同态加密算法和分支程序同态加密算法.

在已有的同态加密算法中,文献[25-27,29]中提出的同态加密算法是对2种或2种以上的运算保持同态的加密方案,用文献[31-34]的同态加密方案加密的密文随着计算乘法或加法电路深度的增加而指数增加.上述方案[25-27,29,31-34]都可以归类到Polly Cracker框架方案[25],该框架系统内所有算法的安全性都是基于理想(ideal)成员资格判定问题,即给定一个环(ring)及其一个理想I和2个元素π,ψ,判定$\pi-\psi\in I$?该框架内的算法都假设理想成员资格判定问题是困难的,但对于这个问题的困难性假设是否成立还有许多疑问[14].此外这些方案的密文膨胀也是一个严重问题[14],因为这种膨胀速度有时甚至是电路深度的双指数(double exponential)函数[14,35],文献[36]对同态加密进行了综述.

2.3 电路全同态

2.1节和2.2节所述的多数概率同态加密算法存在的主要问题都是密文中存在错误,而且错误随着同态运算次数的增加而迅速累积以至于无法正确解密,因此这些算法允许进行同态加密运算的次数都是非常有限的.所以,如何控制错误的积累使得经过多次同态运算仍然能够正确解密就成了同态加密研究的一个核心问题.概率同态加密算法的另一个问题是密文膨胀问题(cipher-text expansion).Gentry[14]分析了Polly Cracker框架方案的优缺点并提出了一种新的全同态加密算法,这种新的全同态加密算法的主要贡献在于通过重复使用bootstrapping实现"用后一个密钥加密用前一个密钥加密过的密文,消除前一个密钥加密的效果和密文中蕴含的错误信息",即在不解密的前提下,将用pk_1加密m的密文$E(pk_1,m)$转换成用pk_2加密m的密文$E(pk_2,m)$,并消除$E(pk_1,m)$中的错误,因而可以进行任意多次的同态加密操作而保证正确解密,理论上可以实现加密存储与密文计算.Gentry算法一经提出,立即得到全世界密码学界的高度重视.这种新的全同态加密方案的理论意义毫无疑问是非常重大的,但要将其应用于实际还有许多困难要克服.

要在实际应用中实现Gentry算法,必须解决下列问题[37]:1)由于密文的长度和加密解密操作的计算复杂度随着操作次数的增加而迅速增加,应用Gentry算法之前必须预先确定同态加密操作的次数,这极其不便;2)为了使同态加密能够进行,算法中不断引入新的没有经过充分论证的假设[38],如近似最大公约数问题假设(approximate greatest common divisor assumption)、电路安全问题假设(circular-secure problem assumption)、稀疏子集和问题假设(sparse subset sum problem assumption)等,有研究认为稀疏子集和问题并不是困难问题[39],所以算法安全性赖以保证的计算困难性问题没有经过充分的论证,算法的安全性还需要进一步的研究.

Gentry同态加密方案的另一个问题是其加解密运算是用电路来表示的,称为电路同态(circuit homomorphy)加密算法,它仅对能够转换成电路的函数有效.虽然理论上任何一个函数都与一个电路等价,并且函数和电路可以互相转化,因此在理论上任何计算都可以表示成一系列加法和乘法组成的布尔电路,一个电路同态加密算法只要对加法和乘法是同态的,就可以进行任何同态加密计算,就可以认为是全同态的.但实际中,要将一个非常简单的计算机程序或者函数转换成等价的布尔电路都很困难,转换后的电路也非常复杂.关于Gentry同态加密算法的复杂度,据Cooney估计[40],仅利用同态加密的关键词进行搜索就使得搜索时间增加10^{12}倍.即使摩尔定律永远没有极限(事实上摩尔定律已经接近极限),摩尔定律再连续作用40年后所制造的处理器运行算法的速度才能达到可以接受的程度,所以电路全同态加密算法目前还无法应用于解决云存储与云计算中的实际安全问题.因此,如何使全同态加密能够在实际中应用是国际密码学界目前最为活跃的研究领域之一,国际上正在掀起分析、研究、优化、

改进全同态加密算法的热潮,但近期看不到实际应用的可能.

Gentry 在文献[41]中提出了一个不需要 bootstrapping 的全同态加密算法,其他学者也相继提出了一些全同态加密算法:文献[42]对 Gentry 的 bootstrapping 电路全同态加密算法进行了改进;文献[43]提出用短密钥提高计算效率的方法;文献[44]提出了建立在近似格问题上的新的全同态加密算法;文献[45]提出了整数基础上的全同态加密算法;文献[46]提出了基于带误差学习(learning with errors)假设的、用重线性化(re-linearize)技术实现的比较高效的全同态加密算法,但每次只能加密 1 b;文献[47]提出了改进同态加密算法的 2 种途径.

上面这些改进算法与新提出的全同态加密算法都是电路全同态的,由于电路全同态加密算法目前都存在难于克服的不足,因此要使这些算法能够在实际中应用都有很长的路要走.

2.4 明文保密计算

用户让自己以明文形式保存的机密数据参与云计算过程,如何保证机密性的问题,理论上讲也可以先采用同态加密的方法对明文数据加密,然后进行密文计算实现保密.但这种做法用户需要先加密再用云进行计算,加密运算可能比用户原本要进行的实际计算还复杂.用户这样做实际是用复杂的计算换取简单的计算,增加了不必要的计算开销,显然是不划算的,因而失去了实际意义.因此应该研究更好的办法来解决这个问题,这时采用明文保密计算(secure plain-text computation)技术保证计算过程的机密性是一种可行的方法.

明文保密计算的思想是 Feigenbaum 在文献[48]中提出的,但她没有用明文保密计算这个术语.本文作者为了便于与密文计算对照而提出了这个术语.以明文方式存储的机密数据,如果不加密而直接利用云服务器进行计算就不能保证数据的机密性.要保证机密性就需要对明文进行适当的加工,然后再利用云进行计算,这就是明文保密计算.明文保密计算与密文计算都是要解决机密数据在计算过程中的保密性问题,它们的区别在于机密数据参与计算时处于不同的存储状态.如果机密数据本身是以密文形式存储的,在此基础上不进行解密直接利用云服务器进行有关的计算,就是密文计算;如果数据是明文存储的,对明文进行保密加工后利用云进行有关的计算,就是明文保密计算.如 2.1 节和 2.2 节所述,密文计算主要是利用同态加密算法保证数据的机密性.

明文保密计算研究方面,Feigenbaum 研究了离散对数计算、二次剩余以及本原根计算问题的解决方案[48].Naor 与 Pinkas[49]利用不经意传输解决了多项式函数的明文保密计算问题,但该方案的计算复杂性很高.本文作者[50-51]研究了保密数字签名问题和几个科学计算问题的明文保密计算.在实际明文保密计算中需要解决的问题多种多样,对于还没有研究过的函数的明文保密计算,有些可以借助多方保密计算已有的研究成果来解决,但大多数函数计算目前还没有相关研究,所以迫切需要针对不同的计算函数研究相应的解决方案或者构造通用的解决方案.

目前明文保密计算的文献还很少,作者认为明文保密计算是保证以明文形式存储的机密数据在云计算过程中机密性的有效技术,对于解决云计算中机密性保护问题有重要的实际意义,是很有前途的研究方向.

3 同态加密的应用

本节对于同态加密的实际应用情况进行简单地总结.同态加密在密文计算方面的重要应用,是同态加密最基本、最重要的应用,这项应用可以使我们不需要信赖云服务商,而利用云服务商的计算能力和存储能力完成需要执行的计算与存储任务,即计算外包和存储外包,基本可以解决云计算与云存储中数据的机密性保护问题,对于云服务的普及有重要的理论与实际意义.除此之外,同态加密在其他方面也有极其广泛的应用:

1) 私有数据银行(private data bank).Rivest,Adleman 和 Dertouzous[6]在提出同态加密概念时就预言同态加密可以用于建立私有数据银行.所谓私有数据银行就是用户可以将自己的数据加密后保存在一个不信任的服务器中,此后可以向服务器查询所需要的信息,服务器生成一个用用户的公钥加密的查询结果,用户可以解密该结果获得自己需要的信息,而服务器并不知道用户具体查询的内容.

2) 加密搜索(encrypted search).用目前已有的电路全同态加密算法可以实现这样的加密搜索过程[14]:用户选择一个全同态加密方案,为该方案生成一个公钥 pk.用 pk 加密要查询的内容 $b_1,b_2,\cdots,b_n$(b_i 可以是用户查询内容的单个比特),生成相应的密文 $c_1,c_2,\cdots,c_n$.假设电路 C 表示搜索引擎的查

询函数,搜索引擎利用同态性计算

$$c_i^* = Evaluate(pk, C_i, (c_1, c_2, \cdots, c_n)),$$

其中 C_i 是电路集合 C 的子电路(sub-circuit),用于计算输出的第 i 比特;$Evaluate()$ 是某个确定的算法.搜索服务器把这些结果发送给用户,用户用私钥 sk 解密 c_i 得到 $C_i(b_1, b_2, \cdots, b_n)$.这些值构成了用户的搜索答案,而搜索引擎不知道用户搜索的真正内容.当然如果能够设计出代数全同态加密算法,这种加密搜索的意义将更大.

3) 在多方保密计算方面的应用.所谓多方保密计算是指 $n(n \geqslant 2)$ 个参与者 $P_1, P_2, \cdots, P_n$ 分别拥有保密数据 $x_1, x_2, \cdots, x_n$,他们希望联合计算函数 $f(x_1, x_2, \cdots, x_n)$,但都不愿意泄露自己的保密数据.多方保密计算是网络隐私保护的关键技术,在密码学与信息安全中有重要的理论与实际意义.现实中的许多游戏(如扑克游戏等)都可以用多方保密计算协议来描述,而许多密码学协议(如秘密共享协议、密钥分配协议、不经意传输协议等)都可以看作是一种特殊的多方保密计算协议.因此多方保密计算也是密码学研究的热点问题,而同态加密算法是构造多方保密计算协议的有力工具.

Bendlin 等人[52]论述了同态加密与多方保密计算的关系,Gentry[14]也详细论述了同态加密在多方保密计算方面的应用.Freedman 等人[53]利用同态加密解决集合相交问题的多方保密计算;Lin 和 Tzeng[54]利用同态加密解决著名的"百万富翁"问题;Du 等人[55]用同态加密解决保密的计算几何问题;Goethals 等人[56]用同态加密解决向量点积的多方保密计算问题;文献[57]用同态加密来解决一般的多方保密计算问题、更多的应用可以查阅文献[14].

4) 其他方面的应用.同态加密在密码学的各个方面都有应用,例如密钥分配、不经意传输、零知识证明等.除此之外还有一些其他的应用,比如 Goldreich 和 Ostrovsky[58]研究了同态加密在软件保护方面的应用;Ostrovsky 和 Skeith[59]设想用同态加密算法可以实现下面的混淆(obfuscation)功能:Alice 首先编写一个程序 P 并加密得到 $E(P)$,然后发送给 Bob,Bob 为程序提供一个输入 x,运行加密后的程序 $E(P)$ 可以得到 $P(x)$;同态加密在代理重加密(proxy re-encryption)中也获得了广泛的应用[14];同态加密可以用于构造零知识证明协议[14],也可以用于构造密钥认证协商协议[60]与代理重加密[61]协议.同态加密还有许多零星的应用,在此不再赘述.

4 公开问题与研究课题

综上所述,对于云服务中数据机密性保护这个主要安全问题,亟需加强以下 9 个方面的研究:

1) 对现有的全同态加密算法,特别是 Gentry 全同态加密算法的数学基础进行分析,这项工作相当于对同态加密算法进行密码分析.由于 Gentry 算法在设计过程中采用了很多新的没有经过充分论证的计算复杂性假设,在算法设计中假设近似最大公约数问题、稀疏子集和问题等是困难的,但这些问题是否真的是困难问题还有待于从数学上做进一步研究.如果经过充分研究从数学上证明这些问题确实是困难的,那么 Gentry 全同态加密算法就是安全的,就可以放心使用;反之如果这些问题并不困难(不是平均意义下的 NP 完全问题),算法就是不安全的.要评价 Gentry 算法是否安全,需要对这些问题作充分的研究.另外,计算困难问题也是设计密码算法的基础,如果这些计算问题确实是困难的,那么它们也可以用在设计其他密码学算法中,因而需要对 Gentry 同态加密算法的数学基础进行深入的研究.

2) 代数全同态加密算法的设计问题.对于电路计算表现为同态的加密算法称为电路同态加密算法(circuit homomorphic encryption algorithm),直接对代数运算表现为同态的算法称为代数同态加密算法(algebraic homomorphic encryption algorithm).现有全同态加密算法基本上都是电路全同态加密算法.借助电路计算理论研究全同态加密的好处是能使问题简单化,这种研究方法的不足是设计的算法不便于实际应用.如果要用电路全同态加密算法实现同态加密,必须把要进行的代数运算转化为相应的计算电路才能实现,但是即使将一个非常简单的运算转化成一个计算电路都是一项非常艰巨的任务.代数全同态加密算法不需要作任何更改,就可以直接应用于实际代数运算,而任何运算都可以转化为代数运算.因此,要在云存储与云计算中利用全同态加密算法解决有关安全问题,必须研究高效的代数全同态加密算法.研究代数全同态加密算法将是云服务安全问题获得解决的关键,是今后一段时间内研究的热点,这个问题也是同态加密算法研究中最为困难的问题.

3) 计算复杂度与密文膨胀问题.现有的代数部分同态加密算法都需要以大整数为模进行模指数运

算,计算复杂性很高.如何降低现有部分代数同态加密算法的计算复杂度、提高计算效率,将成为今后同态加密算法研究的一个重点.密文膨胀问题是所有建立在公钥基础上的语义安全的同态加密算法,即概率同态加密算法本身固有的问题.因为概率加密是从明文空间到密文空间的一对多映射(一个明文有若干可能的密文),所以密文空间一定大于明文空间.现有的所有代数同态加密算法都有密文膨胀问题,理论上不可能完全消除密文膨胀,只能尽量降低密文膨胀率.人们认为有效的概率加密算法的膨胀率应该小于2.最初的概率同态加密算法[12]的密文比明文要长得多(膨胀率大于100),前面提到的很多同态加密算法实际上主要是围绕如何减少密文长度(降低膨胀率)而逐步改进的,但在减少密文膨胀的同时却增加了计算复杂性.各种同态加密算法的密文膨胀率的数据可参阅文献[36].研究如何降低密文的膨胀率,对于同态加密算法的实际应用具有重要的意义.

4)研究更多的构造同态加密算法的困难问题与同态加密方案的构造方法,即研究密码编码的基础和编码方法.对现有各种公钥密码算法的构造方法、数学基础进行全面分析,从中寻求可以用于构造全同态加密算法的计算困难问题;从数学理论中寻找新的可以用于构造同态加密算法的新的计算困难问题,探索利用新的计算困难性假设如Weil双线性对(bilinear pairing)方案[62]、最短向量问题(shortest vector problem)[63]、理想成员问题(ideal membership problem)[64]、带误差学习问题(learning with errors)[46]、线性码问题以及传统的因子分解、离散对数、随机性等问题设计新的高效的同态加密算法.这些计算困难性问题有的已经在同态加密算法设计中得到应用,有的只是在密码学中得到应用,有些还没有找到密码学应用,需要广泛开展这方面的基础研究.

5)研究基于对称密码学理论的同态加密算法.目前的同态加密算法,无论是电路同态加密算法还是代数同态加密算法基本上都是用公钥算法构建的,而所有公钥算法的一个明显缺点是算法的计算复杂性都很高,加密速度很慢.以加密来看AES这种对称分组密码算法的加密速度比RSA公钥加密算法加密快100倍,解密速度比RSA解密快2 000倍.因而通常情况下公钥加密算法不适合大量数据的加密,要实现密文计算就迫切需要研究复杂度低的同态加密算法.已经有学者在这方面进行过一些探索研究[28],探索的成果表明,设计基于对称密码学的同态加密算法也是可能的.

6)在云计算机密性保护的研究中对于明文保密计算的研究还没有引起足够的重视,需要加强这方面的研究工作.理论上代数全同态加密算法可以解决云计算与云存储中的主要安全问题,但以明文形式保存在用户自己的存储设备中的机密数据要参与云计算,利用同态加密进行密文计算就会出现前面所提出的困境:即用户加密$x_1,x_2,\cdots,x_n$的计算开销远比自己计算$F(x_1,x_2,\cdots,x_n)$的计算开销大,因而利用关系

$$G(K,F,(E(x_1),\cdots,E(x_n))) = E(K,F(x_1,\cdots,x_n))$$

获得$F(x_1,x_2,\cdots,x_n)$就变得毫无意义.这种困境需要采用明文保密计算的方法克服.而利用明文保密计算的计算量远远小于同态加密进行保密计算的计算量,但这方面的成果很少,没有现成的方法可以遵循.多方保密计算方面的许多研究成果可以为明文保密计算的研究提供借鉴.明文保密计算也是保证云计算安全的核心技术,因此还须进一步加强这方面的研究.

7)同态加密算法和密文计算算法的计算复杂性分析和性能评价问题.目前已经有多种代数部分同态加密算法以及一些电路全同态加密算法和密文计算算法.代数同态加密算法的计算复杂性要远远低于电路同态加密算法,因此作者认为不需要在代数同态加密算法和电路同态加密算法之间进行计算复杂性的比较.代数部分同态加密算法很多,也是更便于实际应用的算法.在实际应用中非常需要了解各种算法的优劣,特别是对其安全性和计算复杂性进行比较,用于指导在实际应用中合理选择算法.算法的计算复杂性分析还可以为降低算法的复杂度指明方向,但目前基本还没有对各种算法的计算复杂性和性能评价进行研究,因此需要加强这方面的研究.为了进行性能分析,需要为算法制定评价指标体系,并根据指标体系对算法进行全面的评价,为算法的比较和选择提供指导.

8)同态加密算法的局限性.同态加密算法在安全性方面也有一些局限:①同态加密算法不能抵抗自适应选择密文攻击,它能达到的最高安全级别是抵抗选择明文攻击;②可关联性(malleability)是同态加密算法本身固有的性能,所以同态加密算法不能用于要求抵抗自适应密文攻击的场合,也不能用于一些需要具有不可关联(non-malleability[65])方

案支持的应用场合.

保密拍卖需要不可关联承诺方案作为支撑算法,这就决定了同态加密算法不可能用于这种场合.因此对于同态加密方案的局限性要进行研究,清楚了解同态加密方案的适用范围,搞清楚哪些应用可以采用同态加密方案,哪些应用要避免同态加密算法,以免误用同态加密算法而造成安全隐患.

9) 研究同态加密的新应用. 如前所述,同态加密的应用非常广泛,还有很多新的应用等待开拓. 同态加密在云计算和云存储中的应用有待人们进一步研究;同态加密也可以用于解决更多的多方保密计算问题,利用同态加密的性质,对于很多多方保密计算问题可以设计出更有效的协议,这方面有很多问题值得研究. 除此之外,还应该寻求同态加密的一些尚没有发现的新用途. 此外提高同态加密算法的实际实现效率也是值得研究的实际问题.

5 结 论

云服务中的安全问题很多,机密性保护问题是其中最重要的一个方面,从密码学角度看解决云计算与云存储中机密性保护问题的最主要技术是同态加密技术. 本文总结了各种代数部分同态加密算法和电路全同态加密算法的研究现状与研究展望,同时简单介绍了明文保密计算的概念与研究课题. 目前的电路全同态加密算法还只有理论价值,尚不能用于解决实际的密文计算问题,所以高效的代数全同态加密算法构造是同态加密今后的主要研究方向. 如果能够找到高效的代数全同态加密算法,实际密文计算的问题就可以迎刃而解,从而解决云计算与云存储安全中一个最基础、最重要的问题,就可以实现云服务安全的突破. 这对于云服务的研究与普及、对于我国 IT 业的发展和信息化建设都有重大的意义. 在明文保密计算方面我们还没有成熟的理论和方案构造方法,但是在许多方面可以借助于多方保密计算的理论成果来解决明文保密计算方案的理论问题与方案构造问题,这方面也有大量的研究工作要做.

参 考 文 献

[1] Armbrust M, Fox A, Griffith R, et al. Above the clouds: A Berkeley view of cloud computing [EB/OL]. [2014-07-02]. http://x-integrate.de/x-in-cms.nsf/id/DE_Von_Regenmachern_und_Wolkenbruechen_-_Impact_2009_Nachlese/MYMfile/abovetheclouds.pdf

[2] Harauz J, Kaufman L M, Potter B. Data security in the world of cloud computing [J]. IEEE Security & Privacy, 2009, 7(4): 61-64

[3] Feng Dengguo, Zhang Min, Zhang Yan, et al. Study on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83 (in Chinese)
(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)

[4] McMillan R. Cloud computing a 'security nightmare', says Cisco CEO [EB/OL]. [2014-07-02]. http://www.networkworld.comnews/2009/042309-cloud-computing-a-security-nightmare.html

[5] Virvilis N, Dritsas S, Gritzalis D. Secure cloud storage: Available infrastructures and architectures review and evaluation [G] //LNCS 6863: Proc of Trust, Privacy and Security in Digital Business. Berlin: Springer, 2011: 74-85

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

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

[8] Rappe R. Homomorphic cryptosystems and their applications [D]. Dortmund, Germany: University of Dortmund, 2004

[9] 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

[10] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [G] //LNCS 1592: Proc of Eurocrypt'99. Berlin: Springer, 1999: 223-238

[11] Benaloh J. Verifiable scret-ballot elections [D]. New Haven, CT: Department of Computer Science, Yale University, 1988

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

[13] Savage J E. Models of Computation: Exploring the Power of Computing [M]. Reading, MA: Addison-Wesley, 1998

[14] Gentry C. A fully homomorphic encryption scheme [D]. Stanford, CA: Stanford University, 2009

[15] Bendlin R, Damgard I, Orlandi C, et al. Semi-homomorphic encryption and multiparty computation [G] //LNCS 6632: Proc of Eurocrypt 2011. Berlin: Springer, 2011: 169-188

[16] Goldwasser S. Multi-party computations: Past and present [C] //Proc of the 6th Annual ACM Symp on Principles of Distributed Computing. New York: ACM, 1997: 1-6

[17] Du Wenliang, Atallah M J. Secure multi-party computation problems and their applications: A review and open problems [C] //Proc of 2001 Workshop on New Security Paradigms. New York: ACM, 2001: 13-22

[18] Goldreich O. Foundations of Cryptography: Basic Applications [M]. Cambridge, UK: Cambridge University Press, 2004

[19] Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multi-authority election scheme [G] // LNCS 1233: Proc of Eurocrypt'97. Berlin: Springer, 1997: 103-118

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

[21] Okamoto T, Uchiyama S. A new public-key cryptosystem as secure as factoring [G] //LNCS 1403: Proc of Eurocrypt'98. Berlin: Springer, 1998: 308-318

[22] Damgard I, Jurik M. A length-flexible threshold cryptosystem with applications [G] //LNCS 2727: Proc of the 8th Australasian Conf on Information Security and Privacy. Berlin: Springer, 2003: 350-356

[23] Dam W V, Hallgren S, Ip L. Quantum algorithms for some hidden shift problems [J]. SIAM Journal of Computing, 2006, 36(3): 763-778

[24] Boneh D, Goh E J, Nissim K. Evaluating 2-DNF formulas on ciphertexts [G] //LNCS 3378: Proc of 2005 Theory of Cryptography Conf. Berlin: Springer, 2005: 325-341

[25] Fellows M, Koblitz N. Combinatorial cryptosystems galore [G] //LNCS 1122: Proc of the 2nd Int Symp on Finite Fields. Berlin: Springer, 1993: 51-61

[26] Melchor C A, Gaborit P, Herranz J. Additively homomorphic encryption with t-operand multiplications [G] //LNCS 6223: Proc of CRYPTO 2010. Berlin: Springer, 2010: 138-154

[27] Ajtai M, Kumar R, Sivakumar D. A sieve algorithm for the shortest lattice vector problem [C] //Proc of Symp on Theory of Computing(STOC'01). New York: ACM, 2001: 601-610

[28] Dijk M V. Interval obfuscation, MIT-CSAIL-2009 [R]. Cambridge, MA: MIT Press, 2009

[29] Sander T, Young A, Yung M. Non-interactive crypto-computing for NC [C] //Proc of FOCS'99. Piscataway, NJ: IEEE, 1999: 554-567

[30] Ishai Y, Paskin A. Evaluating branching programs on encrypted data [G] //LNCS 4392: Proc of TCC'07. Berlin: Springer, 2007: 575-594

[31] Beaver D. Minimal-latency secure function evaluation [G] // LNCS 1807: Proc of Eurocrypt 2000. Berlin: Springer, 2000: 335-350

[32] Vehel F L, Perret L. A polly cracker system based on satisfiability [J]. Coding, Cryptography and Combinatorics, 2003, 23: 177-192

[33] Ly L. A public-key cryptosystem based on polly cracker [D]. Bochum, North Rhine-Westphalia, Germany: Ruhr Universität Bochum, 2002

[34] Ly L. Polly two: A new algebraic polynomial-based public-key scheme [J]. Applicable Algebra in Engineering, Communication and Computing, 2006, 17(3/4): 267-283

[35] Wikipedia. Double exponential function [EB/OL]. [2014-07-12]. http://en. wikipedia. org/wiki/Double __ exponential function

[36] Fontaine C, Galand F. A survey of homomorphic encryption for non-specialists [EB/OL]. [2014-07-12]. http://jis. eurasipjournals. com/content/2007/1/013801

[37] Schneier B. Homomorphic encryption breakthrough [EB/OL]. [2014-07-12]. http://www. schneier. com /blog/ archives/2009/07/homomorphic_enc. html

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

[39] Lee M S. On the sparse subset sum problem from Gentry-Halevi's implementation of fully homomorphic encryption [EB/OL]. [2014-07-12]. http://eprint. iacr. org/2011/567. pdf

[40] Cooney M. IBM touts encryption innovation [EB/OL]. [2014-07-12]. http://www. computerworld. com/s/article/ 9134823/IBM_touts_encryption_innovation?taxonomyId=152&intsrc=kc_top&taxonomyName=compliance

[41] Brakerski Z, Gentry C. Fully homomorphic encryption without bootstrapping [EB/OL]. [2012-07-12]. http: // eprint. iacr. org/2011/277. pdf

[42] Stehle D, Steinfeld R. Faster fully homomorphic encryption [G] //LNCS 6477: Proc of the 16th Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2010: 377-394

[43] Coron J S, Mandal A, Naccache D, et al. Fully homomorphic encryption over the integers with shorter public keys [G] //LNCS 6841: Proc of Crypto 2011. Berlin: Springer, 2011: 487-504

[44] Gu Chunsheng. New fully homomorphic encryption over the integers [EB/OL]. [2014-07-12]. http://eprint. iacr. org/ 2011/118. pdf

[45] Dijk M V, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [G] //LNCS 6110: Proc of Eurocrypt 2010. Berlin: Springer, 2010: 24-43

[46] Brakerski Z, Vaikuntanathany V. Fully homomorphic encryption from ring-LWE and security for key dependent messages [G] //LNCS 6841: Proc of Crypto 2011. Berlin: Springer, 2011: 505-524

[47] Lauter K, Naehrig M, Vaikuntanathan V. Can homomorphic encryption be practical [C] //Proc of the 3rd ACM Workshop on Cloud Computing Security. New York: ACM, 2011: 113-124

[48] Feigenbaum J. Can You take advantage of someone without having to trust him [G] //LNCS 218: Proc of Crypto'85. Berlin: Springer, 1986: 477-488

[49] Naor M, Pinkas B. Oblivious polynomial evaluation [J]. SIAM Journal on Computing, 2006, 35(5): 1254-1281

[50] Li Shundong. Three specific secure computation service protocols [J]. Journal of Shaanxi Normal University, 2010, 38(4): 1-6 (in Chinese)
(**李顺东. 三个保密计算服务协议[J]. 陕西师范大学学报**, 2010, 38(4): 1-6)

[51] Li Shundong, Wang Daoshun, Dai Yiqi. Secure signature protocol [J]. Intelligent Information Management, 2009, 1 (3): 174-79

[52] Bendlin R, Damgard I, Orlandi C, et al. Semi-homomorphic encryption and multiparty computation [G] //LNCS 6632: Proc of Eurocrypt 2011. Berlin: Springer, 2011: 169-188

[53] Freedman M J, Nissim K, Pinkas B. Efficient private matching and set intersection [G] //LNCS 3027: Proc of Eurocrypt 2004. Berlin: Springer, 2004: 1-19

[54] Lin Hsiaoying, Tzeng Wenguey. An efficient solution to the millionaires' problem based on homomorphic encryption [G] //LNCS 3531: Proc of the 3rd Int Conf on Applied Cryptography and Network Security. Berlin: Springer, 2005: 456-466

[55] Atallah M J, Du Wenliang. Secure multi-party computational geometry [G] //LNCS 2125: Proc of the 7th Int Workshop on Algorithms and Data Structures. Berlin: Springer, 2001: 165-179

[56] Goethals B, Laur S, Lipmaa H, et al. On private scalar product computation for privacy-preserving data mining [G] //LNCS 3506: Proc of the 7th Int Conf on Information Security and Cryptology. Berlin: Springer, 2005: 104-120

[57] Damgard I, Pastro V, Smart N, et al. Multiparty computation from somewhat homomorphic encryption [EB/OL]. [2014-07-02]. http://eprint. iacr. org/2011/535. pdf

[58] Goldreich O, Ostrovsky R. Software protection and simulation by oblivious RAMs [J]. Journal of the ACM, 1996, 43(3): 431-473

[59] Ostrovsky R, Skeith W E. Private searching on streaming data [G] //LNCS 3621: Proc of Crypto 2005. Berlin: Springer, 2005: 223-240

[60] Gao Haiying. Provable secure ID-based authenticated key agreement protocol [J]. Journal of Computer Research and Development, 2012, 49(8): 1685-1690 (in Chinese)
(高海英. 可证明安全的基于身份的认证秘要协商协议[J]. 计算机研究与发展, 2012, 49(8): 1685-1690)

[61] Guo Lifeng, Lu Bo. Efficient proxy re-encryption with keyword search scheme. Journal of Computer Research and Development, 2014, 51(6): 1221-1229 (in Chinese)
(郭丽峰, 卢波. 有效的带关键字搜索的代理重加密[J]. 计算机研究与发展, 2014, 51(6): 1221-1229)

[62] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [J]. SIAM Journal of Computing, 2003, 32(3): 586-615

[63] Peikert C. Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract [C] //Proc of the 41st Annual ACM Symp on Theory of Computing. New York: ACM, 2009: 333-342

[64] Arvind V, Mukhopadhyay P. The ideal membership problem and polynomial identity testing [J]. Information and Computation, 2010, 208(4): 351-363

[65] Dolev D, Dwork C, Naor M. Non-malleable cryptography [C] //Proc of the 23rd ACM Annual Symp on the Theory of Computing(STOC'91). New York: ACM, 1991: 542-552

Li Shundong, born in 1963. PhD, professor, and PhD supervisor of Shaanxi Normal University. Member of China Computer Federation. His main research interests include cryptography and information security, correctness proof of programs, e-commerce.

Dou Jiawei, born in 1963. PhD, associate professor of Shaanxi Normal University. Her main research interests include applied mathematics, application of cryptography.

Wang Daoshun, born in 1964. PhD, associate professor, and PhD supervisor of Tsinghua University. Member of China Computer Federation. His research interests include visual cryptography, information hiding and digital water-marking (daoshun@tsinghua.edu.cn).