DOI:10.3969/j.issn.1009-6868.2016.01.006
http://www.cnki.net/kcms/detail/34.1228.TN.20151225.0953.002.html

安全多方计算技术研究与应用

Research and Application of Secure Multi-Party Computation

张卷美/ZHANG Juanmei
徐荣华/XU Ronghua
(北京电子科技学院,北京 100070)
(Beijing Electronic Technology Institute, Beijing 100070, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2016) 01-0023-003

摘要: 认为同态密码的本质是通过密文运算,实现相对应的明文运算。基于同态密码、格理论密码,分别设计了安全多方计算协议,解决了安全两方线段求解直线相交问题和聚类分析中一种经常遇到的加权平均问题。认为目前安全多方计算的实际应用比较滞后,但随着其理论的不断成熟以及各种密码理论基础技术的不断发展,安全多方计算最终会为新时代下的信息安全提供服务。

关键词: 安全多方计算;同态加密;格密码

Abstract: The essence of homomorphic encryption is to realize the corresponding plaintext operation by calculating cipher text. In this paper, we propose some secure multi-party computation schemes based on homomorphic encryption and lattice theory. With these protocols, the secure two-party line segment intersection problem and weighted-average problem, which are often encountered when solving the problem of clustering analysis, are solved. Practical application of secure multi-party computation is lagging, but with the continuous development of its theory and various kinds of cryptography, secure multi-party computation will increase information security in the future.

Key words: secure multi-party computation; homomorphic encryption; lattice homomorphism

安全多方计算是密码学的基础问题之一,概括了大多数密码协议,如认证协议、在线支付协议、公平交换协议、拍卖协议、选举协议、密文数据库查询与统计等等。在电子选举、电子投票、秘密共享等场景有关广泛的应用[1-2]。

1 安全多方计算的概念

针对安全多方计算,2004年Goldreich给出了一个简单、完整、统一形式化定义[3]。他将安全多方计算抽象成一个随机过程:U_1、U_2、……、U_n是n互不信任的参与方,共同计算函数$f(x_1,x_2,\cdots,x_n)=(y_1,y_2,\cdots,y_n)$,其中函数$f$是一个计算复杂度为概率多项式的随机函数,$U_i$拥有秘密输入$x_i\in(0,1)^*$,通过计算希望获得$y_i\in(0,1)^*$,但不向其他参与方泄露任何信息。

在理想的世界中,假设第三方是可信的,计算函数f,则其计算时间亦为概率多项式时间,抽象为交互式图灵机,其执行过程为可信第三方收集各方输入,然后计算结果,再分别秘密发送结果给对应参与方。理想世界中敌手IA执行协议过程中获取到的输出变量为$IDEAL(\mathrm{IA})$。

在现实的世界中,可信第三方不存在,同样计算函数f,则需要收集各方输入,然后计算输出结果,再分别秘密发送结果给对应参与方。理想世界不同的是敌手RA可以窃听并收集诚实参与方之间的通信信息,但不能修改其通信内容。现实世界中敌手IA执行协议过程中获取到的输出变量为$REAL(\mathrm{RA})$。

对于现实世界中的任意敌手RA,都存在相应理想敌手IS,若在计算过程中,使得$IDEAL(\mathrm{IA})$和$REAL(\mathrm{RA})$计算不可区分,即$IDEAL(\mathrm{IA})\approx REAL(\mathrm{RA})$,则认为安全多方计算协议是安全的。

2 同态加密理论在安全多方计算中的应用

同态加密[4]能够在不对密文解密的情况下,对密文进行计算,从而实现对明文的计算,这与安全多方计算中在不泄露任何数据隐私信息的情况下完成安全计算的需求不谋而合。

目前,同态密码是密码学领域研究的热点之一。同态的分类较为常见的是:单同态、双同态、无限同态和有限同态,这是一个较为概括性的分类方法。

(1)单同态是指关于明文的某一种运算具有同态特性的同态,分为乘法同态和加法同态。

收稿日期:2015-11-20
网络出版时间:2015-12-25

• 乘法同态

对于加密体制 $ALG(E,D,P,C)$，$x\in P$，$y\in P$，如果满足 $D(E(x)@E(y))=xy$（@为密文空间 C 的操作），则称 ALG 满足乘法同态。

• 加法同态

对于加密体制 $ALG(E,D,P,C)$，$x\in P$，$y\in P$，如果满足 $D(E(x)\#E(y))=xy$（#为密文空间 C 的操作），则该体制 ALG 满足加法同态。

（2）双同态指关于明文空间的加法运算和乘法运算都是同态的，且明文空间必须是一个环。

（3）全同态指关于明文空间可以实现任何运算的同态，即对明文空间的任何运算都可以转化为密文空间恰当的运算解密值。无限的双同态密码体制，可以转化为全同态。

通过对现有的具有同态性质的加密体制进行分析，我们得出：原始的ElGamal加密体制满足乘法同态、RSA满足加法同态、Paillier满足加法同态等。虽然目前没有成熟易用的同态密码体制能够满足任意形式的计算需求，但是已经存在的成熟且具有单一同态性质的密码算法就能够满足部分安全多方计算场景中的应用[5-6]。

利用具有加法同态密码体制可以求解百万富翁问题。两个富翁分别为A和B，并且有一个满足加密的同态加密算法 $ALG(E,D,P,C)$，假设A的财富为 m_1，B的财富为 m_2，分别用加密算法对财富进行加密：$E(m_1)=M_1$，$E(m_2)=M_2$，得出 (M_1,M_2) 的大小就可以得到 (m_1,m_2) 的大小。因为 $D(E(m_1)-E(m_2))=m_1-m_2$。

我们利用ElGamal密码体制可以求解两私有点的直线方程问题，实际上就是要秘密求出两私有点坐标差商的问题。这就是著名的安全两方线段求交问题。

在求解之前，我们先设计一个新的ElGamal密码体制。

（1）系统参数为：选择一个大的素数 p，g 是循环群 Z_p^* 的生成元，再选一个随机数 $x\in Z_p^*$，计算 $y=g^x \bmod p$，私钥为 x，公钥为 (y,g,p)。

（2）加密过程为：对任意的消息 m，选随机数 k，满足 $\gcd(p-1)=1$，计算密文 $E(m)=(a,b)=(g^k \bmod p, y^k g^m \bmod p)$。

（3）解密过程为：计算 $\log_g(b/(a)^x)\bmod p$，得到明文。

显然，求对数要付出很大的计算代价，需要在 Z_p^* 的空间里搜索结果。本方案用预先计算，查表解密的方法实现。上述密码算法有加法同态特性。假设 (m_1,m_2) 为两个消息：

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

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

在密文空间定义一种预算 $E(m_1)@E(m_2)=(a_1a_2 \bmod p, b_1b_2 \bmod p)$，则有：

$$E(m_1)@E(m_2)=(g^{k_1+k_2} \bmod p, y^{k_1+k_2} g^{m_1+m_2} \bmod p) \quad (1)$$

显然，$D(E(m_1)@E(m_2))=m_1+m_2 \bmod p$ 满足加法同态特性。

上述密码体制满足与常数 n 的乘法同态性下文称为常数乘法同态，也可以理解为一种特殊的求 n 次和的加法同态，则有：

$$\begin{aligned} D(E(m)^n) &= D(E(m)@E(m)@\cdots@E(m)) \\ &= D(g^{nk} \bmod p, y^{nk} g^{nm}) \bmod p \\ &= nm \bmod p \end{aligned} \quad (2)$$

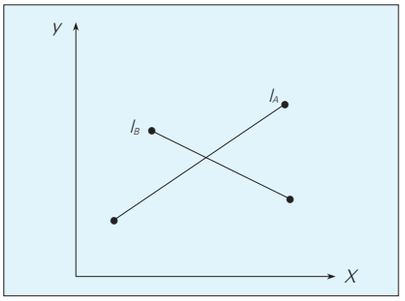
在安全两方线段求交问题中，假设Alice拥有线段 $l_A: y=a_1x+b_1 \bmod p$，Bob拥有线段 $l_B: y=a_2x+b_2 \bmod p$。Alice和Bob希望计算两条线段的交点。计算结束后，除了交点的坐标信息外，对方不能获知其他任何信息，如图1所示。

上述问题的实质就是求解式(3)。

$$\begin{cases} y=a_1x+b_1 \\ y=a_2x+b_2 \end{cases}$$ 其中：

$$m_1\leqslant x\leqslant n_1,\ m_2\leqslant x\leqslant n_2 \quad (3)$$

当 $a_1-a_2\neq 0$ 时，解为 $x=\dfrac{b_2-b_1}{a_1-a_2}$，$y=a_1x+b_1$



▲图1 安全两方线段求解直线相交问题

安全多方计算协议[7]设计为：Alice拥有 (a_1,b_1)，对应密文为 $A(E(a_1),E(b_1))$；Bob拥有线段 (a_2,b_2)，对应的密文为 $B(E(a_2),E(b_2))$。

利用上述新设计的密码体制，通过密文计算可以得 $x=\dfrac{r(b_2-b_1)}{r(a_1-a_2)}=\dfrac{b_2-b_1}{a_1-a_2}$，并可得出安全两方线段的交点：$(\dfrac{b_2-b_1}{a_1-a_2}, a_1x+b_1)$。

类似于这样的问题还有很多，如判断3个私有点共线问题等，这些问题都可以采用该协议来解决。

3 格理论在安全多方计算中的应用

格理论的研究源自于1611年Kepler所提出的猜想。经过400多年的发展，格的困难问题依次被提出来，最后确定了格上的主要困难问题：最短向量问题（SVP）、最近向量问题（CVP）、小整数解问题（SIS）、错误学习问题（LWE）等。早期的格理论主要应用于密码分析，如1982年Lenstra等提出的LLL格基规约算法，该算法能够有效求解出近似于最短向量的格基。直到1996年，Ajtai证明了在最坏情况下与平均情况下求解格困难问题是等价的，并给了设计格密码方案新的想法，这对于研究格密码方案具有重要的意义。

格理论上的安全多方计算协议是基于格公钥密码体制，NTRU公钥密码体制是一种基于格的公钥密码体制。

（1）系统参数为：3个公开参数为

(N,p,q)，通常情况下 $p=3,q=2^k$，$N-1$ 是多项式的最高次数，$*$ 表示卷积乘，设 $a(x),b(x)\in R$，则 $c(x)=a(x)*b(x)=\sum_{k=0}^{N-1}[\sum_{i+j=k \bmod N} a_i b_j]x^k$。它构建在商环 $Z[x]/(x^N-1)$ 上。$L(a,b)$ 表示环中具有 a 个系数为1，b 个系数为-1，其余系数均为0的全体整系数多项式。随机选取两个多项式 $f=1+pF$ 和 $g\in L(d_g,d_g)$，其中保证 f 存在逆元 f_p 和 f_q，使得 $f\times f_p=1(\mathrm{mod}\,p)$，$f\times f_q=1(\mathrm{mod}\,q)$。计算 $h=f_q\times g(\mathrm{mod}\,q)$，NTRU的公钥为 (N,p,q,h)，私钥为 f。

（2）加密过程为：用户选取随机多项式 $r\in L(d_r,d_r)$，对于明文消息 m，计算 $c=pr*h+m(\mathrm{mod}\,q)$ 得到密文。

（3）解密过程为：解密者得到密文 $c=pr\times h+m(\mathrm{mod}\,q)$ 后，首先计算 $a\equiv c\times f(\mathrm{mod}\,q)$，再计算 $m'=a\times f_p$，最后计算 $m\equiv m'(\mathrm{mod}\,p)$。

因为 $E(x)+E(z)=p(r_1+r_2)h+(x+z)(\mathrm{mod}\,q)$，令 $r_5=r_1+r_2$，则可得出：

$$E(x)+E(z)=pr_5h+(x+z)(\mathrm{mod}\,q)=E(x+z) \quad (4)$$

因此NTRU公钥加密体制满足加法同态性质。

又因为 $E(x)=pr_1h+x(\mathrm{mod}\,q)$，$z\times E(x)=pzr_2h+zx(\mathrm{mod}\,q)$，令 $r_6=x*r_2$，则可得出：

$$z\times E_A(x)=E_A(zx) \quad (5)$$

因此，可以认为NTRU公钥加密体制满足乘法混合同态性质。

聚类分析中有一种常用遇到的是加权平均问题（WAP），该问题描述为：A拥有 (x,m)，其中 x 为一实数，m 是一个整数；B拥有 (y,n)，希望能够联合计算 $\frac{x+y}{m+n}$。在加权平均问题中，整数 n 和 m 需要被保护，双方需要在不知对方任何消息的条件下，联合完成计算，并且需要保证计算结果的正确性。

上述加权平均问题已在文献[8]中给予解决。文中假设有 n 个用户 $(P_1,P_2,\cdots,P_n)$，每个用户拥有 (x_i,y_i)（其中 $i=1,2,\cdots,n$），安全计算为 $\frac{x_1+x_2+\cdots+x_n}{y_1+y_2+\cdots+y_n}$。

假设参与安全多方计算的用户分别为 $P_1,P_2,\cdots,P_n$，选取 P_n 作为最终结果的计算者，基于NTRU设计的多方安全计算协议流程如下：

（1）P_n 选取可逆多项式 z，通过采用文献[9]两方安全计算协议，可从 P_1 处得到 $z(x_1+x_n)$ 和 $z(y_1+y_n)$，从 P_i 处得到 $z(x_i+x_n)$ 和 $z(y_i+y_n)$，$(i=1,2,\cdots,n)$。

（2）结合收集到的数据，P_n 采用NTRU体制的加法同态性将所有数据相加，计算得到 $z(x_1+x_2+\cdots+n\times x_n)$ 和 $z(y_1+y_2+\cdots+n\times y_n)$。

（3）计算 $z(x_1+x_2+\cdots+n\times x_n)-(n-1)\times z\times x_n=z(x_1+x_2+\cdots+x_n)$，采用同样的方法得到 $z(y_1+y_2+\cdots+y_n)$。

（4）计算得到 $\frac{x_1+x_2+\cdots+x_n}{y_1+y_2+\cdots+y_n}$。

（5）将 $E_{P_i}(\frac{x_1+x_2+\cdots+x_n}{y_1+y_2+\cdots+y_n})$ 发送给用户 P_i，其中 $i=i,2,\cdots,n$。

（6）各个用户通过解密可以获得将 $\frac{x_1+x_2+\cdots+x_n}{y_1+y_2+\cdots+y_n}$。

上述安全多方计算协议借助交互多方中的某一位成员进行计算，其他成员只与该成员进行交互，最终计算方将所得结果秘密传送给各个成员。该方案类似于单方交互协议，可以最终实现安全多方计算，但是在效率上有待提高。

4 结束语

作为密码学研究的一个重要方向，安全多方计算既古老又年轻。与理论研究成果相比，安全多方计算的实际应用比较滞后，主要是效率和安全性还不能完全满足现实的需求。根据安全多方计算的特点，我们已经为各种不同的应用场景设计了相应的安全多方计算方案，主要集中在大数据隐私保护、云计算和文数据库检索和统计等安全性需求较高的应用场景中。未来还有很多研究要做，主要集中在恶意型下的多方安全计算问题中，因为恶意模型环境下参与方可以完全不遵守协议规则。虽然在现阶段，安全多方计算的应用还存在困难，但是随着安全多方计算理论的不断成熟以及各种密码理论基础技术的不断应用，安全多方计算最终会走入我们的实际生活，为互联网时代、云计算时代、大数据时代的信息安全服务。

参考文献

[1] YAO Q Z. Protocols for Secure Computations [C]// Proceedings of 23rd Annual IEEE Symposium on Foundations of Computer Science，Chicago, USA, 1982: 160– 164
[2] GOLDREICH O, MICALI S, WIGDERSON A. How to Play Any Mental Game or A Completeness Theorem for Protocols with Honest Majority [C]//STOC 1987, 1987: 218–229
[3] GOLDREICH O. Foundations of Cryptography: Volume II – Basic Applications [M]. Britain: Cambridge University Press, 2004
[4] GENTRY C. A Fully Homomorphic Encryption Scheme [D]. USA: Stanford University, 2009
[5] DU W L. Secure Multiparty Computation Problems and Their Applications[C]//A Review and Open Problems New Security Paradigms Workshop 2001, Cloudcroft , New Mexico, USA, 2001
[6] 刘文, 王永滨. 安全多方信息比较相等协议及其应用[J]. 电子学报, 2012, 40(5): 871–876
[7] 陈志伟，张卷美，李子臣. 基于ElGamal变体同态的安全两方计算协议设计[J]. 通信学报, 2015, 36(2): 1–8
[8] 刘立强，李子臣.一种基于NTRU的安全两方计算协议[C]//全国信息隐藏暨多媒体信息安全学术大会（CIHW），北京, 中国, 2012
[9] 胡予濮. 一个新型的NTRU类数字签名方案[J]. 计算机学报, 2008, 31(9): 1661–1666

作者简介

张卷美，北京电子科技学院基础部副教授；从事计算数学的教学和研究工作；主持参加省级学术研究、教改项目6项；发表学术论文和教改论文20余篇，编写出版教材5部。

徐荣华，北京电子科技学院基础部教师，长期从事代数、密码学教学与科研等工作。