doi:10.11959/j.issn.1000-436x.2015050

基于 ElGamal 变体同态的安全两方计算协议设计

陈志伟[1]，张卷美[2]，李子臣[2]
（1. 数据通信科学技术研究所，北京 100191；2. 北京电子科技学院 信息安全系，北京 100070）

摘 要：本文分析了 ElGamal 的同态特性，针对协议设计需要，设计了 ElGamal 变体加密方案，使其满足加法同态和常数乘法同态。在半诚实模型下，基于这个变体提出了过私有点直线方程同态计算协议，并分析了协议的正确性、安全性、计算和通信复杂性，同时将该协议的应用范围扩展到安全两方线段求交协议等。与解决同类几何问题的协议相比，未采用基于不经意传输和百万富翁协议设计思路，而是基于同态加密体制提出了一种安全两方计算协议，提高了该类协议的执行效率，降低了通信负担。
关键词：安全两方计算；同态加密；ElGamal 加密体制；私有点计算
中图分类号：TP918.1 **文献标识码**：A

Design for secure two-party computation protocol based on ElGamal variant's homomorphic

CHEN Zhi-wei[1], ZHANG Juan-mei[2], LI Zi-chen[2]
(1. Data Communication Science & Technology Research Institute, Beijing 100191, China;
2. Department of Information Security, Beijing Electronic Science & Technology Institute, Beijing 100070, China)

Abstract: ElGamal homomorphic characteristics were analyzed. In order to meet the need of protocol design, ElGamal variant was designed, which satisfies additive homomorphism and constant multiplication homomorphism. A homomorphism calculate protocol of linear equation passed by two private point based on the ElGamal variant was also proposed, then the correctness, security and the complexity of computation and communication of the protocol were analyzed to extend the application of thinking to secure two-party line segments intersection scheme. Compared with the similar protocol of solving the geometric problem, a kind of secure two-party computation protocol based on homomorphic encryption system without using the oblivious transfer protocol and the millionaires protocol was put forward, which holds higher efficiency and a lower burden of communication.
Key words: secure two-party computation; homomorphic encryption; ElGamal encryption system; private point calculation

1 引言

同态加密机制是基于秘密同态的概念，是秘密同态的一个子集。秘密同态的思想由 Rivest 等[1]提出，即在不解密密文的条件下，通过对密文执行操作做到对明文数据的各种计算。2009 年，冠以密码学圣杯的“全同态加密”被 Gentry[2]提出的基于理想格的全同态方案所实现，方案基于理想格，提出了一套能够自举的 Somewhat 同态加密算法，这里，“Somewhat”是指同时满足乘法同态和加法同态的双同态密码体制。然后，通过自举技术中的扩大电路、噪声约减实现 Somewhat 同态到全同态的转换。虽然该方案效率较低，无法实现真正的实际应用，但是，这是第一次从实际意义上实现了全同态的概念，极大地推动了全同态密码体制的研究进展，也使全同态加密成为国内外学者研究的重点领域。同

收稿日期：2013-07-31；**修回日期**：2014-03-19
基金项目：国家自然科学基金资助项目（61070219, 61370188）；中央高校基本科研业务费专向基金资助项目
Foundation Items: The National Natural Science Foundation of China (61070219, 61370188); The Fundamental Research Funds for the Central Universities

态加密的一个重要应用就是安全多方计算，所谓安全多方计算是指：一组参与者希望共同计算某个约定的函数，每个参与者为要解决的函数提供一个输入，出于安全考虑，要求参与者的输入不能对其他人泄露。倘若存在安全可信第三方(TTP, trusted third party)，则安全多方协议所要解决的问题就能够得到解决。这时，只需各参与者将各自的输入交给 TTP，由 TTP 来计算出函数值，再将计算结果公布给各参与者。但现实中很难找到这样的 TTP,，从而安全的两方计算协议显得尤为重要，目前安全多方计算已得到许多学者的研究，其在密码学上的地位也日益重要，它是电子选举、权值分摊、电子拍卖等密码学协议的基础。目前，对于安全多方计算协议的研究主要集中在协议的设计方面。Yao[3]于 1982 年首次提出了安全的两方计算协议。后来，Goldreich 等[4]对安全多方计算做了比较完整的总结，并提出了证明安全多方计算安全性的方法。密码学家 Goldwasser[5]总结了多方计算的本质就是多个用户在不泄露自己秘密的情况下，以自己的秘密作为输入，共同计算某个函数。

同态加密体制能够在不解密的情况下实现对密文的计算，这与安全两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一致。虽然没有有效的全同态加密算法，但是已经存在的成熟且具有单一同态性质的密码算法（RSA、ElGamal、Paillier、Bresson 等）就能够满足部分安全多方计算场景中的应用。

用安全多方计算思想来解决安全几何问题是安全多方计算的另一个重要应用领域，Du 等[6,7]提出了一系列的可以用安全多方计算思路来解决的安全几何计算问题，包括：几何点的包含问题，几何图形的相交问题、保密点的凸壳问题、安全两方线段的求交问题。但是当时作者并未给出合理的安全性证明和计算复杂性分析。为了叙述方便，提出一类私有点计算问题的解决思路，为了形象地说明本文要解决的安全多方计算问题，首先考虑如下场景。A 军、B 军是战争中的盟军，但是互不知晓对方的位置。现在要确定一条经过 A、B 的航线，如何在不泄露 A 和 B 位置信息的情况下求出这条直线的方程。本文就是围绕这 2 个私有点计算问题展开讨论，最终设计出了能够解决这类问题的安全两方计算方案。

上述问题的本质就是如何根据 2 个点位置的密文求出通过两私有点直线的问题。类似于此问题的私有点安全多方计算问题并不是一个新的概念，国内外学者已经设计出了多种私有点的两方计算协议。文献[6]提出了一种基于不经意传输协议(OT, oblivious transfer)的确定私有直线交点的算法。但是，这些方案需要 n 选 1 的 OT 协议，增加了计算的复杂度和复杂大量随机数生成的过程。文献[8]提出了安全多方信息（例如，私有点位置）比较相等问题，提出了一个不泄露任何额外信息的安全多方信息比较相等协议，但是该协议计算复杂度和通信复杂度仍较高。文献[9]基于向量差最小值协议和同态加密方案，实现了安全多方最近点对协议，协议的效率高于文献[8]，且不需要不经意传输协议的参与。文献[10]基于 Graham 算法、安全叉积协议、姚氏百万富翁协议设计了一个新型的安全两方凸分组求解算法。Wang 等在文献[11]中对上述求解算法进行了新的改进，基于裹包法、百万富翁协议、叉积协议解决了安全两方凸分组问题。文献[12]运用 Paillier 同态密码体制和姚氏百万富翁问题解决了安全两方线段求交点协议，该方案是同态加密体制的一个较好应用。本文采用了该文的同态加密思路，直接采用 ElGamal 变体的同态性，与文献[6,8,9,11,12]相比，在既不采用 n 选 1 的 OT 协议，也不使用姚氏百万富翁协议的条件下，解决了本文提出的两私有点直线方程求解问题。

原始 ElGamal 仅具备乘法同态，本文通过对 ElGamal 的改进，设计了 ElGamal 变体加密方案，该方案不仅具有更强的安全性，而且满足加法同态，同时能够执行常数乘的同态运算，这样使 ElGamal 变体能够执行通过对密文的操作实现明文计算的需求。采用 ElGamal 变体的安全两方计算协议不再采用传统的 OT 协议和百万富翁协议，降低了通信次数与计算复杂度，大大提高了协议的执行效率。同态加密的应用使本协议性能优于同类判定协议。

2　预备知识

2.1　相关定义

定义 1　计算模型。安全两方计算是一种安全的分布式计算协议，在该协议中，2 个成员 A 与 B 分别持有各自的秘密输入 x 与 y，对某个特定的函数 f，他们希望计算函数值 $f(x,y)$，但 A 与 B 都不愿意向对方泄露出自己的输入。在计算过程中，一

般 A 与 B 首先对各自的输入进行伪装，映射成另一个数据，然后两方在伪装后的数据上进行计算，最后将计算的中间结果还原成原问题的解，如图 1 所示。

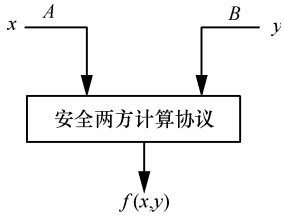

图 1 安全两方计算模型

定义 2 私有点计算问题。私有点是指二维坐标系中，坐标位置为 $(x_1,\cdots,x_n,y_1,\cdots,y_n)$，为了安全，位置加密为 $(E(x_1),\cdots,E(x_n),E(y_1),\cdots,E(y_n))$。而在实际应用中，又需要坐标值参与一些问题的计算，如何在不泄露点坐标信息的情况下，完成这些计算的问题，被称为私有点计算问题。

定义 3 两私有点直线方程求解问题。私有点直线方程求解问题是指如何在不泄露 2 个私有点明文信息的情况下，求得通过这 2 个私有点的方程问题。

定义 4 半诚实参与者。一个半诚实参与者是指安全多方运算中一个参与计算的用户，能严格执行协议的规程，不会中途强行退出或恶意掺入虚假数据，但在协议执行过程中他可能会保留所有能搜集到的关于对方的信息，以期望在协议结束后计算出对方的输入数据。

定义 5 概率多项式时间（PPT, probability polynomial time）在密码学安全模型中，协议的参与者处于同步网络环境中，并通过不安全的信道通信，协议的参与者和攻击者的计算能力受限于 PPT。

2.2 半诚实模型下的两方安全计算定义

安全多方计算的目的就是保证多方计算协议的安全性。目前，广泛应用的安全性分析方法是 Goldreich 在文献[13]提出的，该定义相比以前的分析方法更加严格和完备。证明方法首先定义了一个存在 PPT 的理想模型，在执行过程中，如果真实协议遇到的所有攻击都能够在理想模型下重现，那么就认为该协议是安全的。通过 Goldreich 证明方法对协议的安全性进行证明，证明的方法可以描述如下。

定义 6 半诚实模型下的两方协议的安全性。设：$f:\{0,1\}_1^*\times\{0,1\}_m^*\to\{0,1\}_1^*\times\{0,1\}_m^*$ 为泛函，其中，$f_1(x,y)$ ($f_2(x,y)$)记为 $f(x,y)$ 的第一元素（第二元素）。令 Π 为计算 f 的两方协议，第一方（第二方）在输入为 (x,y) 时 Π 执行过程中的视图（View）标记 $VIEW_1^{\Pi}(x,y)$（$VIEW_2^{\Pi}(x,y)$），即 $(x,r,m_1,\cdots,m_t)$，（$(y,r,m_1,\cdots,m_t)$），其中 r 为第一方（第二方）内部掷币过程的输出，m_i 为参与方接收到的第 i 个消息。在协议 Π 执行完毕后，第一方（第二方）基于输入 (x,y) 的输出记为 $OUTPUT_1^{\Pi}(x,y)$（$OUTPUT_2^{\Pi}(x,y)$），显然输出包含在参与者的视图中，且有：$OUTPUT^{\Pi}(x,y)=(OUTPUT_1^{\Pi}(x,y),OUTPUT_2^{\Pi}(x,y))$。

确定情况：对一个确定的函数 f，称 Π 秘密地计算了 f，如果存在 PPT 算法分别标记为 S_1 和 S_2，且使得以下等式成立

$$\{S_1(x,f_1(x,y))\}_{x,y\in(0,1)^*}\overset{c}{\equiv}VIEW_1^{\Pi}(x,y)_{x,y\in(0,1)^*} \tag{1}$$

$$\{S_2(x,f_2(x,y))\}_{x,y\in(0,1)^*}\overset{c}{\equiv}VIEW_2^{\Pi}(x,y)_{x,y\in(0,1)^*} \tag{2}$$

其中，$|x|=|y|$，$\overset{c}{\equiv}$ 表示多项式电路族计算不可区分。

一般情况：称 Π 秘密地计算了 f，如果存在 PPT 算法分别标记为 S_1 和 S_2，且使得以下等式成立

$$\{S_1(x,f_1(x,y),f(x,y))\}_{x,y\in(0,1)^*}\overset{c}{\equiv}\{VIEW_1^{\Pi}\cdot (x,y)_{x,y\in(0,1)^*},OUTPUT_1^{\Pi}(x,y)_{x,y\in(0,1)^*}\}_{x,y} \tag{3}$$

$$\{S_2(x,f_2(x,y),f(x,y))\}_{x,y\in(0,1)^*}\overset{c}{\equiv}\{VIEW_2^{\Pi}\cdot (x,y)_{x,y\in(0,1)^*},OUTPUT_2^{\Pi}(x,y)_{x,y\in(0,1)^*}\}_{x,y} \tag{4}$$

这里需要强调的 $VIEW_1^{\Pi}(x,y)$、$VIEW_2^{\Pi}(x,y)$、$OUTPUT_1^{\Pi}(x,y)$、$OUTPUT_2^{\Pi}(x,y)$ 为相关的随机变量，由相同的随机执行函数定义。特别地，$OUTPUT_i^{\Pi}(x,y)$ 完全由 $VIEW_i^{\Pi}(x,y)$ 确定。

确定情况下的两方视图，基于任何可能的输入，都能被自己输入和输出有效地模拟。相应地，一般情况下两方视图，就必须考虑计算函数是随机的，$OUTPUT^{\Pi}(x,y)=f(x,y)$ 不一定成立，因为两者都是随机的，这时要求协议的输出与 $f(x,y)$ 有相同的分布。确定情况是一般情况的一种特殊情况，本文设计协议的证明是在一般情况下，因此具有更强的安全性。

该定义可以直观地理解为对于一个半诚实参与者，如果可以直接利用自己的输入与协议的输出

通过构造的模拟器 S_1 和 S_2，执行协议的过程，进而得到过程中所能得到的输出，那么协议就能保证输入的私密性。如果一个计算协议能被这样模拟，参与者就不能从协议的执行过程中得到有价值的信息，这样的协议就是安全的。

2.3　同态加密

同态加密的思想由 Rivest 等在文献[1]中提出，即在不解密密文的条件下，通过对密文执行操作，就能够做到对明文数据的各种计算。1998 年，Sander 等在文献[14]中定义了整数环上的加法、乘法同态加密机（HES, homomorphic encryption scheme），来确保 2 个变量加密后的计算结果与加密前的计算结果相同。胡予濮老师[15]在报告中总结了同态的分类，提出了他的分类方法，即同态可以分为：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经典分类方法。

单同态指关于明文乘法或加法运算的同态。“大数分解”陷门的公钥加密原型和“离散对数”陷门的公钥加密原型都只能实现单同态，且这个单同态是无限的，即任意多个明文的加法运算都是对应密文的乘法运算的解密值。

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。基于一些“译码难题”陷门的公钥加密方案可以实现双同态，且这个双同态是有限的，即少量明文的环运算是对应密文的环运算的解密值。常见的译码难题包括格上的难题，且陷门的公钥加密方案是带有误差的方案，误差尺寸在一定限度之内才能被正确解密。

全同态指关于明文空间可以实现任何的运算的同态，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分析，如 ElGamal 满足单一的乘法同态、RSA 满足单一的乘法同态、Paillier 满足单一的加法同态[16]、Bresson 满足单一的加法同态等。最终通过对 ElGamal 密码体制的改造实现了协议设计所需要的重要一步，即加法同态操作后乘以常数 r 的混淆和计算，大大提高了协议的运行效率和安全性，实现了单同态体制下的安全两方计算协议。

2.4　“ElGamal 变体”同态性分析

ElGamal 既可用于数字签名又可用于加密[17]，其安全性依赖于循环群上计算离散对数问题的困难性和 Diffie-Hellman 假设。ElGamal 密码体制满足乘法同态，然而协议计算两点间差的时候，需要用到加法同态，原始 ElGamal 就不能满足要求。所以本文设计了一个 ElGamal 的变体方案，使其满足加法同态，也能够进行常数乘法的同态运算，ElGamal 变体的设计可以描述如下。

1) 选择一个大的素数 p，$g(g<p)$ 是循环群 Z_p^* 的生成元，选一个随机数 $x\in Z_p^*$，计算 $y=g^x \bmod p$。公钥 (y,g,p,α)，g 和 p 可由一组用户共享，私钥为 x。

2) 加密。选随机数 k，与 $p-1$ 互素，密文：$E(M)=(a,b)=g^k \bmod p,\ y^k\alpha^M \bmod p$。

3) 解密。明文的幂值为：$\alpha^M=b(a^x)^{-1} \bmod p$，进而求对数得到：$M=\log_\alpha \alpha^M$。虽然，求对数要付出很大的计算代价，需要在 α^M 的空间里搜索结果，但是通过 Pollard lambda 的方案[18]能够平均减少搜索范围至 $c\alpha^{\frac{M}{2}}$，减少了计算耗时。

4) 加同态。加密消息 M_1，$M_2(M_1+M_2<p)$。密文

$$E(M_1)=(a_1,b_1)=(g^{k_1} \bmod p, y^{k_1}\alpha^{M_1} \bmod p)$$

$$E(M_2)=(a_2,b_2)=(g^{k_2} \bmod p, y^{k_2}\alpha^{M_2} \bmod p)$$

如果定义 $E(M_1)\otimes E(M_2)=(a_1a_2,b_1b_2)$，则有 $E(M_1)\otimes E(M_2)=(g^{k_1+k_2} \bmod p, y^{k_1+k_2}\alpha^{(M_1+M_2)} \bmod p)$ $=g^{k_1+k_2} \bmod p,\ y^{k_1+k_2}\alpha^M \bmod p$。其中 $M=M_1+M_2$，则 $D(E(M_1)\oplus E(M_2))=M_1+M_2$，即具有加同态特性，同时满足求与常数 n 乘积的运算（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）

$$\begin{aligned}&(E(M_1)\otimes E(M_2))^n=((g^{k_1+k_2})^n \bmod p,\\&(y^{k_1+k_2}\alpha^{(M_1+M_2)})^n \bmod p)\\&=(g^{n(k_1+k_2)} \bmod p, y^{n(k_1+k_2)}\alpha^{n(M_1+M_2)} \bmod p)\end{aligned}$$

解密可得：$n(M_1+M_2)$。

3　求过私有点直线方程协议设计

3.1　问题分析

为了形象地说明问题，以 A 军、B 军为例，首先虚拟一个大型的地理位置二维坐标系，如图 2 所示，

A 军拥有自己位置信息 $A(x_A,y_A)$，经过 ElGamal 变体加密的密文坐标信息 $A'(E(x_A),E(y_A))$；B 军拥有自己位置信息 $B(x_B,y_B)$，采用 A 军的 ElGamal 变体公钥对其坐标进行加密得到：$B'(E(x_B),E(y_B))$。现在要求出通过 A、B 两地的航线，确定航线方程，且又不泄露两地信息。

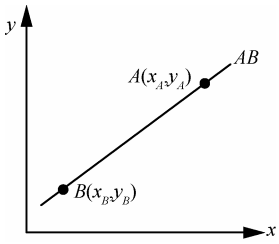

图 2 求私有点直线方程问题描述

简单地描述即在不泄漏 A、B 两点信息的情况下，求经过 A、B 两点的直线。

通过 A、B 两点的直线可以表示为

$$y = k_{AB}x + y_A - k_{AB}x_A \tag{5}$$

其中，$k_{AB} = \dfrac{y_A - y_B}{x_A - x_B}$。

问题的核心，在于两方秘密地求出斜率 k_{AB}，进而完成直线方程的计算。

3.2 协议设计

步骤 1 由 A 军生成通信过程中要用到的 ElGamal 的公私钥，公钥：(y,g,p,α)，私钥：x。

同时将公钥 (y,g,p,α) 传递给 B 军。

步骤 2 A 军计算自己位置坐标的密文值为：$A'(E(x_A),E(y_A))$，并发送给 B 军。B 军采用接收 A 的公钥 (y,g,p,α) 对自己坐标进行加密得：$B'(E(x_B),E(y_B))$。

步骤3 B 军根据收到的 $A'(E(x_A),E(y_A))$ 和自己计算的 $B'(E(x_B),E(y_B))$。首先计算坐标密文的差值

$$E(\Delta y) = (E(y_A) \odot E(y_B)) = E(y_A - y_B) \tag{6}$$

$$E(\Delta x) = (E(x_A) \odot E(x_B)) = E(x_A - x_B) \tag{7}$$

然后，随机生成随机数 r_1。利用 ElGamal 变体的乘法同态计算得

$$E(r_1\Delta y) = (E(y_A - y_B))^{r_1} = E(r_1(y_A - y_B)) \tag{8}$$

$$E(r_1\Delta x) = (E(x_A - x_B))^{r_1} = E(r_1(x_A - x_B)) \tag{9}$$

将 $E(r_1\Delta y)$ 和 $E(r_1\Delta x)$ 传送给 A。

步骤 4 A 根据收到的 $E(r_1\Delta y)$ 和 $E(r_1\Delta x)$，解密得：$D(E(r_1\Delta y)) = D(E(r_1(y_A - y_B))) = r_1(y_A - y_B)$。求得直线斜率

$$k_{AB} = \frac{r_1(y_A - y_B)}{r_1(x_A - x_B)} = \frac{y_A - y_B}{x_A - x_B} \tag{10}$$

计算直线 $l_1 : y = k_{AB}x + y_A - k_{AB}x_A$，则直线 l_1 即为所求。

同理，A 把斜率 k_{AB} 发送给 B，这样 B 便可计算得 $l_2 : y = k_{AB}x + y_B - k_{AB}x_B$，且 $l_1 = l_2$。两轮交互后，A 军和 B 军便得到了两点间的直线方程。

3.3 正确性分析

定理 1 协议能正确求出经过 2 个私有点的直线方程。

证明 证明过程省略了系统初始化部分，且 A 军、B 军位置坐标的密文信息分别为

$$E(A) = [(g^{k_1}, y^{k_1}\alpha^{x_A}),(g^{k_2}, y^{k_2}\alpha^{y_A})] \bmod p \tag{11}$$

$$E(B) = [(g^{k_3}, y^{k_3}\alpha^{x_B}),(g^{k_4}, y^{k_4}\alpha^{y_B})] \bmod p \tag{12}$$

以 A、B 两军为例，B 军根据密文信息后计算

$$E(\Delta y) = (E(y_A) \odot E(y_B)) = \frac{(g^{k_2}, y^{k_2}\alpha^{y_A})}{(g^{k_4}, y^{k_4}\alpha^{y_B})} \bmod p$$

$$= (g^{k_2-k_4}, y^{k_2-k_4}\alpha^{y_A-y_B}) \bmod p \tag{13}$$

将差值加入随机数 r_1，

$$\begin{aligned} E(r_1\Delta y) &= (E(y_A))^{r_1} \\ &= \left((g^{k_2-k_4}, y^{k_2-k_4}\alpha^{y_A-y_B})\right)^{r_1} \bmod p \\ &= \left((g^{k_2-k_4}, y^{k_2-k_4}\alpha^{y_A-y_B})\right)^{r_1} \bmod p \\ &= \left(g^{r_1(k_2-k_4)}, y^{r_1(k_2-k_4)}\alpha^{r_1(y_A-y_B)}\right) \bmod p \\ &= E(r_1(y_A - y_B)) = E(r_1\Delta y) \end{aligned} \tag{14}$$

将 $E(r_1\Delta y)$ 发送给 A 军，A 军进行解密可得

$$\begin{aligned} D(E(r_1\Delta y)) &= \frac{y^{r_1(k_2-k_4)}\alpha^{r_1(y_A-y_B)}}{(g^{r_1(k_2-k_4)})^x} = \left(\frac{y^{k_2-k_4}\alpha^{y_A-y_B}}{g^{xk_2-xk_4}}\right)^{r_1} \\ &= \left(\frac{y^{k_2}}{g^{xk_2}}\frac{g^{xk_4}}{y^{k_4}}\alpha^{y_A-y_B}\right)^{r_1} = \alpha^{r_1(y_A-y_B)} \end{aligned} \tag{15}$$

最后，以 α 为底取对数便得 $r_1(y_A - y_B)$。同理，A、B 军可以得到 $r_1(x_A - x_B)$。可得到斜率 k_{AB} 即为

$$k_{AB} = \frac{r_1(y_A - y_B)}{r_1(x_A - x_B)} = \frac{y_A - y_B}{x_A - x_B} \tag{16}$$

A 军便得到了直线方程：$y = k_{AB}x + y_A - k_{AB}x_A$。$A$ 将斜率 k_{AB} 发送给 B，这样 A 和 B 就得到了过两点的

直线方程。整个过程中，并没有泄漏任何秘密信息，且完成了经过两点直线的计算，正确性得证。

3.4 安全性分析

安全多方计算的安全类型可以按敌手计算能力的大小而分为：无条件安全和计算安全。无条件安全，又名信息论安全，指敌手拥有无限计算能力时仍然具有的安全性。计算安全，又名密码学安全，安全性的前提是敌手的计算能力受限于 PPT。本文主要从密码学安全的角度去分析协议的安全性。

定理 2　在半诚实模型下，上述协议是安全的。

证明　通过构造预备知识里的符合 2.2 节中式(3)和式(4)的模拟器来证明方案的安全性，且由于上述协议的关键在于求斜率 k_{AB}，A 军输入位置坐标的密文信息为：$E(A)=[E(x_B),E(y_A)]\bmod p$。$B$ 军输入位置坐标的密文信息为：$E(A)=[E(x_B),E(y_A)]\bmod p$。

A 在执行 $\prod$ 的过程中视图(view)记为：$view_A^{\Pi}(A,B)=view_A^{\Pi}(A,pk,sk,E(x_A),E(y_A),k_{AB}B,r_1,E(y_B),E(y_B)),E(r_1(x_A-x_B)),E(r_1(y_A-y_B)))$。

输出：$output_A^{\Pi}(A,pk,sk,E(x_A),E(y_A),k_{AB},B,r_1,E(y_B),E(y_B),E(r_1(x_A-x_B)),E(r_1(y_A-y_B)))=k_{AB}$。

下面构造模拟器 S 模拟 A 军协议的执行过程。

步骤 1　模拟器 S 的输入为：$S(A,f_1(A,B),f_2(A,B))=\{A,pk,sk,E(x_A),E(y_A),k_{AB},f_1(A,pk,E(x_A),E(y_A),B,E(r_1(x_A-x_B)),E(r_1(y_A-y_B))),f_2(sk,E(r_1(x_A-x_B)),E(r_1(y_A-y_B)),k_{AB})\}$。其中，$f_2(sk,E(r_1(x_A-x_B)),E(r_1(y_A-y_B)),k_{AB})=k_{AB}$。

步骤 2　S 利用系统公钥 pk 执行加密操作，可以得到 $E(x_A)$ 和 $E(y_A)$。存在

$$E'(y_A)=E(y_B)\sqrt[r_1]{E(r_1(y_A-y_B))} \tag{17}$$

$$E'(x_A)=E(x_B)\sqrt[r_1]{E(r_1(x_A-x_B))} \tag{18}$$

由于在半诚实模型下，ElGamal 变体同态加密体制是安全的。故有：$E'(y_A)\overset{c}{\equiv}E(y_B)$，$E'(x_A)\overset{c}{\equiv}E(x_B)$。即多项式链路不可区分。$S$ 利用系统私钥 sk 按式(19)计算 k_{AB}。

$$k_{AB}=\frac{D(E(r_1(x_A-x_B)))}{D(E(r_1(y_A-y_B)))} \tag{19}$$

步骤 3　令 $S(A,f_1(A,B))=(A,pk,sk,E(x_A),E(y_A),k_{AB},B,r_1,E(y_B),E(y_B),E(r_1(x_A-x_B)),E(r_1(y_A-y_B)))$。模拟器为：$S(A,f_1(A,B),f_2(A,B))=(A,pk,sk,E(x_A),E(y_A),k_{AB},B,r_1,E(y_B),E(y_B),E(r_1(x_A-x_B)),E(r_1(y_A-y_B)))=k_{AB}$。

视图：$\{view_A^{\Pi}(A,B),output_B^{\Pi}(A,B)\}=\{A,pk,sk,E(x_A),E(y_A),k_{AB},B,r_1,E(y_B),E(y_B),E(r_1(x_A-x_B)),E(r_1(y_A-y_B))\}$。所以，可以构造一个模拟器 S，其中的 $output_B^{\Pi}(A,B)$ 完全由 $view_A^{\Pi}(A,B)$ 来判定且满足等式

$$S(A,f_1(A,B),f_2(A,B))\overset{c}{\equiv}\{view_A^{\Pi}(A,B),output_B^{\Pi}(A,B)\} \tag{20}$$

同理，可以为 B 构造上述的模拟器，本协议在半诚实模型下的安全性得证。

4 讨论

4.1 类似问题的解决

本协议的内容虽然是求解过两私有点的直线方程，但是实际上是要秘密求出两私有点坐标差商的问题。所以，能够把安全多方计算归结到求两私有点坐标差商的问题，都能够通过这个方法解决。这样的问题有著名的安全两方线段求交问题，文献[16,18]均对该问题提出了自己的解决方案，但是执行效率较低。问题的具体描述如下。

A 拥有线段 $l_A:y=a_1x+b_1(m_1\leqslant x\leqslant n_1)$，$B$ 拥有线段 $l_B:y=a_2x+b_2(m_2\leqslant x\leqslant n_2)$。$A$ 和 B 希望计算 2 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，上述问题为安全两方线段求交点问题。解决该问题的协议称为安全两方线段求交协议。

2 条线段在二维空间中的位置，有多种情况，本文仅讨论图 3 所示的情形，即 2 条线段交叉，且交点只有一个的情形。

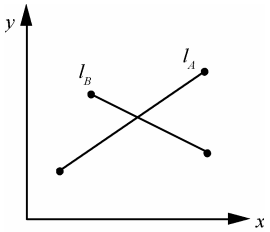

图 3　安全两方线段求交问题描述

上述问题的实质就是求解式(21)在式(22)中的解

$$\begin{cases}y=a_1x+b_1\\ y=a_2x+b_2\end{cases} \tag{21}$$

取值范围：$m_1 \leqslant x \leqslant n_1$，$m_2 \leqslant x \leqslant n_2$ (22)

当 $a_1 - a_2 \neq 0$ 时，式(21)的解为 $x = \dfrac{b_2 - b_1}{a_1 - a_2}$，$y = a_1 x + b_1$。求解 x 的值后验证是否满足式(22)即可。

类似于求斜率的方式，使用上述安全多方计算协议，初始化：A 拥有 (a_1, b_1)，对应密文为 $A(E(a_1), E(b_1))$。B 拥有线段 (a_2, b_2)，对应的密文为 $B(E(a_2), E(b_2))$。

按照 3.2 节中设计的协议即可求出

$$x = \frac{r(b_2 - b_1)}{r(a_1 - a_2)} = \frac{b_2 - b_1}{a_1 - a_2}$$

安全两方线段的交点为：$(\dfrac{b_2 - b_1}{a_1 - a_2}, a_1 x + b_1)$。

类似于这样的问题还有判断 3 个私有点共线问题、求叉积问题[19]等，这些问题都可以采用本文提出的协议来解决。

4.2 性能分析

计算复杂度：本协议中，共执行加密操作 2 次，解密操作 2 次，加密数据的乘法操作 $r_1 + 1$ 次，普通数据乘法操作 1 次。ElGamal 变体加密算法的计算复杂度为 $O(\log p)$，解密算法的复杂度为 $O(\log p)$，每次加密数据的乘法运算复杂度和加密一样也为 $O(\log p)$，且由于采用了 ElGamal 变体的同态特性，使本方案的设计未使用传统的百万富翁协议和 n 选 1 的不经意传输协议，这都在一定程度上减少了计算的复杂度，忽略协议计算过程中的乘法和加法操作，计算复杂度类似于 Sun 在文献[11]提出的计算方法，即在常数 $r = 1$ 时的复杂度为 $O(\log p)$。

通信复杂度：在分布式系统中，通信次数对系统性能影响非常大，本协议中 A 军和 B 军共通信 4 次，由于本文同态加密性质的应用，减少了百万富翁协议和传统方案的 n 选 1 的 OT 协议的交互过程，故通信次数大大减少，使本算法在性能上具有很大的改进。

协议的效率是由计算复杂度和通信复杂度两部分组成，许多文献并没有明确使用哪个具体的算法，这为算法性能的比较带来了一定的不便。本文在进行算法比较时，选用了经典基础算法进行比较。如表 1 所示，C_a 表示百万富翁协议的通信次数，C_c 表示保护隐私的点线叉积协议的通信次数，Y 代表使用，N 代表未使用。

表 1 几种该类型安全多方计算方案的性能对比

文献	计算复杂度	通信复杂度	百万富翁协议	n 选 1 的 OT 协议
本文	$O(\log p)$	4	N	N
文献[12]	$O(r \log N)$	$4 + 3C_a$	Y	N
文献[16]	$O(n^2)$	6	N	Y
文献[19]	$O(n \log N + n^2)$	$4C_a + 4C_c$	Y	Y
文献[20]	$O(C \log N)$	$8 + 3C_a$	Y	N

表 1 给出了与同类型的各方案对比，可见所提协议既未采用不经意传输协议，也未采用解决百万富翁问题的协议，实现了效率的提升，从计算复杂度和通信复杂度上都低于传统方案。与文献[20]相比，在求两私有线段的相交问题上，所提协议不仅能够判断出相交与否，还能直接求出交点。与文献[16,19,20]相比在信道的安全性上，本文采用的是公钥加密，安全性则基于 ElGamal 的离散对数问题，具备更高的安全性。

5 结束语

通过对常见公钥算法同态性的研究，提出了对 ElGamal 的同态性改进，使其具备加法同态和常数乘法同态，进而完成了私有点方程计算协议的设计。在协议的分析阶段，首先，证明了协议的安全性。然后，在 Goldreich 提出的半诚实模型下，验证了协议的安全性。最后，与现有同类型方案的对比发现，通过采用不同于传统设计思路的基于不经意传输和百万富翁协议设计，提出基于同态加密体制的安全两方计算协议，使其具有更高的执行效率，更小的通信负担，降低了计算和通信复杂性。在下一步的研究中，将研究该协议的应用范围，不仅要将其扩展到安全两方线段求交协议中，还要将其应用于其他同类型的安全两方几何计算问题的求解中去。

参考文献：

[1] RIVEST R, ADLEMAN L, DERTOUZOS M. On Data Banks and Privacy Homeomorphisms[M]. In Foundations of Secure Computation, 1978.169-177.

[2] GENTRY C. A Fully Homomorphic Encryption Scheme[D]. Stanford University, 2009.

[3] YAO Q Z. Protocols for secure computations[A]. Proceedings of 23rd Annual IEEE Symposium on Foundations of Computer Science[C]. Los Alamitos: IEEE Computer Society Press, 1982.160- 164.

[4] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game[A]. The 19th Annual ACM Conference on Theory of Computing[C]. New York, 1987.218-229.

[5] GOLDWASSER S. Multiparty computations: past and present[A]. Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing[C]. Santa Barbara, C A, USA, 1997.1-6.

[6] DU W L J A. Secure multiparty computation problems and their applications[A]. A Review and Open Problems New Security Paradigms Workshop 2001[C]. Cloudcroft , New Mexico, USA, 2001.

[7] GENG T, LUO S, XIN Y, *et al*. Research on secure multiparty computational geometry[J]. Information Computing and Applications, 2011. 322-329.

[8] 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.
LIU W, WANG Y B. Secure multi-party comparing protocol and its applications[J]. ACTA Electronica Sinica, 2012, 40(5):871-876.

[9] ZHONG H, SUN Y F, YAN F F, *et al*. Protocol for privacy-preserving space closet-pair of points[J]. Computer Engineering and Applications, 2011, 48 (4):87-89.

[10] LU S F, LUO Y L. Privacy-preserving in graham algorithm for finding convex hulls[J]. Computer Engineering and Application, 2008, 44(36):130-133.

[11] WANG Q, LUO Y L, HUANG L S. Privacy-preserving protocols for finding the convex hulls[A]. ARES' 08[C]. Washington, USA, 2008. 727-732.

[12] SUN M H, LUO S S, *et al*. Secure two-party line segments intersection scheme and its application inprivacy-preserveing convex hull intersection[J]. Journal on Communcatios,2013,34(1): 30-42.

[13] GOLDREICH O. The foundations of cryptography[A]. Basic Applications[C]. Cambridge: Cambridge University Press, 2004.

[14] SANDER T, TSCHUDIN C. Protecting mobile agents against malicious hosts[A]. Proceeding of IEEE Symposium of Research in Security and Privacy 1998[C]. Oakland, California, USA, 1998. 215-224.

[15] 胡予濮. 格上全同态加密[EB/OL]. http://meeting.xidian.edu.cn/html/lectures/201211/324.html.2012.
HU Y P. Fully homomorphic encryption on lattice[EB/OL]. http://meeting. xidian.edu.cn/html/lectures/201211/324.html, 2012.

[16] 罗永龙, 黄刘生, 徐维江等. 一个保护私有信息的多边形相交判定协议[J]. 电子学报, 2007, 35(4): 685-691.
LUO Y L, HUANG L S, XU W J, *et al*. A protocol for privacy-preserving intersect-determination of two polygons[J]. ACTA Electronica Sinica, 2007, 35(4):685-691.

[17] CHEN Z, ZHANG R, LI Z, *et al*. A homomorphic ElGamal variant based on BGN's method[A]. 2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC.2013)[C]. Beijing: IEEE Computer Society Press, 2013.1-5.

[18] 李顺东, 戴一奇, 王道顺等. 几何相交问题的多方保密计算[J]. 清华大学学报, 2007, 47(10): 1692-1695.
LI S D, DAI Y Q, WANG D S, *et al*. Secure multi-party computations of geometric intersections[J]. Journal of Tsinghua University, 2007, 47(10):1692-1695.

[19] 罗永龙, 黄刘生, 荆巍巍等. 保护私有信息的叉积协议及其应用[J]. 计算机学报, 2007, 30(2): 248-254.
LUO Y L, HUANG L S, JING W W, *et al*. Privacy-preserving cross product protocol and its application[J]. Chinese Journal of Computers , 2007, 30(2):248-254.

[20] 刘文, 罗守山, 陈萍. 保护私有信息的点线关系判定协议及其应用[J].北京邮电大学学报, 2008,31(2):72-75.
LIU W, LUO S S, CHEN P. Privacy-preserving point-line relation determination protocol and its application[J]. Journal of Beijing University of Posts and Telecommunications, 2008, 31(2):72-75.

作者简介：

陈志伟（1989-），男，河南周口人，数据通信科学技术研究所工程师，主要研究方向为密码学、云计算、信息安全。

张卷美（1967-），女，河南焦作人，北京电子科技学院副教授，主要研究方向为信息与计算科学、信息安全。

李子臣（1965-），男，河南焦作人，北京电子科技学院教授、博士生导师，主要研究方向为公钥密码学、信息安全、后量子签名理论、云计算等。