软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(12):3274−3292 [doi: 10.13328/j.cnki.jos.005239]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

同态加密方案及安全两点直线计算协议*

巩林明[1,2], 李顺东[2], 窦家维[3], 郭奕旻[2], 王道顺[4]

[1](西安工程大学 计算机科学学院,陕西 西安 710048)

[2](陕西师范大学 计算机科学学院,陕西 西安 710062)

[3](陕西师范大学 数学与信息科学学院,陕西 西安 710062)

[4](清华大学 计算机科学与技术系,北京 100084)

通讯作者: 窦家维, E-mail: jiawei@snnu.edu.cn

摘 要: 近年来,安全多方计算一直是密码领域的一个研究热点,保密几何计算是其一个重要分支.过两私有点坐标安全地计算一条直线问题,在空间信息安全方面有重要应用前景.首先,提出一个由加密方计算(或选取)加密底数的 Paillier 变体同态加密方案,并证明了其在标准模型下对适应性选择明文攻击(adaptive chosen-plaintext attack,简称 CPA)是安全的;然后,在半诚实模型下,基于该变体同态加密方案设计了一个能够安全计算过两私有点直线的协议.还可以将此协议推广应用到可以归约为安全计算两私有点坐标差商的所有安全多方几何计算问题,从而解决了原有的基于同态加密体制的安全两方计算协议存在的信息泄露问题.

关键词: 同态加密;安全多方计算;选择明文攻击;坐标差商

中图法分类号: TP309

中文引用格式: 巩林明,李顺东,窦家维,郭奕旻,王道顺.同态加密方案及安全两点直线计算协议.软件学报,2017,28(12):3274−3292. http://www.jos.org.cn/1000-9825/5239.htm

英文引用格式: Gong LM, Li SD, Dou JW, Guo YM, Wang DS. Homomorphic encryption scheme and a protocol on secure computing a line by two private points. Ruan Jian Xue Bao/Journal of Software, 2017,28(12):3274−3292 (in Chinese). http://www.jos.org.cn/1000-9825/5239.htm

Homomorphic Encryption Scheme and A Protocol on Secure Computing a Line by Two Private Points

GONG Lin-Ming[1,2], LI Shun-Dong[2], DOU Jia-Wei[3], GUO YI-Min[2], WANG Dao-Shun[4]

[1](School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China)

[2](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[3](School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China)

[4](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

Abstract: In recent years, secure multiparty computation is one of research focuses in the field of cryptography, and secret geometry calculation is an important branch of it. The problem of safely calculating a straight line by two private coordinate point has important application prospect in space information security. First, a variant of Paillier's homomorphic encryption scheme is put forward in that the base is calculated by sender during encryption, and its indistinguishability under adaptive chosen-plaintext attack is proved. Then, based on this homomorphic encryption scheme, a protocol that can safely calculate a straight line by two private coordinate point in semi-honesty model is designed. Moreover, this protocol can be applied to solve a type of secure multiparty computational geometry problem that can be reduced to compute coordinate difference quotient. Thus, the problem that there is a non-negligible probability of

* 基金项目: 国家自然科学基金(61272435, 61373020, U1536102)
Foundation item: National Natural Science Foundation of China (61272435, 61373020, U1536102)
收稿时间: 2016-05-03; 修改时间: 2016-09-01, 2016-11-24; 采用时间: 2017-01-09; jos 在线出版时间: 2017-03-24
CNKI 网络优先出版: 2017-03-24 15:31:38, http://kns.cnki.net/kcms/detail/11.2560.TP.20170324.1531.003.html

private information leakage in the current coordinate difference quotient calculation protocols based on homomorphic encryption is solved.

Key words: homomorphic encryption; multiparty secure computation; chosen plaintext attack; coordinate difference quotient

Yao[1]在 1982 年提出了第一个安全两方计算问题,即百万富翁问题,从此产生了安全多方计算(secure multiparty computation,简称 SMC).后来,Goldreich[2]发展丰富了 SMC,并为 SMC 提出了规范的安全性证明模型:模拟范例.安全多方计算从提出到现在的 30 多年中取得了丰硕成果,这些成果按照采用的主要密码学工具大致可以分为基于不经意传输的安全多方计算协议[1,3−6]、基于秘密共享体制的安全多方计算协议[7,8]、基于同态加密体制的安全多方计算协议[9−16].

基于不经意传输的安全多方计算通常在混淆(garbled circuit)电路[1,3−6]上实现.而在电路上实现的安全计算协议的通信复杂度是要保密计算函数的电路深度的常数倍,如果电路规模很大,安全计算协议的效率就很低.

为了避开复杂的混淆电路转换计算,设计高效的、解决具体问题的安全多方计算协议,具有某些特性的密码学工具受到人们的青睐.基于同态加密方案构造的安全多方计算协议较基于秘密共享和不经意传输构造的安全多方计算协议具有如下的良好特性:

- 同态加密支持密文数据计算(可以通过密文上的计算实现参与方私有数据的秘密计算);
- 基本协议设计不需要多秘密验证工作;
- 基本协议设计不需要不经意传输.

因此,同态加密技术成为人们构造高效的、具体的安全多方计算协议时经常采用的一个重要工具.

安全多方几何计算已经成为安全多方计算的一个重要分支,最初由 Du[17]提出,之后,文献[18−23]相继给出了一系列具体、高效的安全多方几何计算问题,包括点与几何图形的位置判定(包含)问题、保密几何的相交问题、保密的凸壳问题、安全两方线段求交点问题、安全多方立体几何计算问题以及陈志伟等人[16]提出的过两点保密计算一条直线的问题.上述问题中,保密计算问题最终都归约为解决多点间对应坐标的保密计算(加、减、乘、除),所以很多具体的安全多方几何计算协议都可以利用同态加密实现.例如,陈志伟等人试图采用改进的 ElGamal 同态加密算法解决一个新的安全两方几何计算问题:A 国、B 国是战争中的一对盟友,两国在海外的秘密军事基地分别驻扎军队 P_1 与 P_2,但是 P_1 与 P_2 互不知晓对方的位置.现在 P_1 与 P_2 要秘密地确定一条经过两方坐标点的航线,而不泄露各方的位置信息.此问题的实质是过两个私有点保密计算一条直线的问题.

陈志伟等人提出的问题是安全多方几何计算问题,在空间信息安全领域很有研究价值.虽然他们设计的协议在执行效率方面显示出了较高的优势,但是该协议存在两方面的不足.

1. 协议会造成(不可忽略的)信息泄露,这是因为:
   - 该协议最终归约到能否安全求解两私有点的坐标差商;
   - 不失一般性,设只有两方参与上述安全几何计算协议,并设两个参与者中拥有同态加密方案私钥一方拥有点$(\mathcal{X}_a,\mathcal{Y}_a)$,另一方拥有点$(\mathcal{X}_b,\mathcal{Y}_b)$.则造成无密钥一方信息泄露的具体原因如下:
     (1) 对于坐标差商的计算,需要先分别计算出分子 $r(\mathcal{Y}_b-\mathcal{Y}_a)$与分母 $r(\mathcal{X}_b-\mathcal{X}_a)$,然后再通过除法将 $r(\mathcal{Y}_b-\mathcal{Y}_a)$与 $r(\mathcal{X}_b-\mathcal{X}_a)$的共有随机数消除,即 $\frac{r(\mathcal{Y}_b-\mathcal{Y}_a)}{r(\mathcal{X}_b-\mathcal{X}_a)}=\frac{\mathcal{Y}_b-\mathcal{Y}_a}{\mathcal{X}_b-\mathcal{X}_a}=\frac{\Delta\mathcal{Y}}{\Delta\mathcal{X}}$;
     (2) 然而,如果$\mathcal{Y}_b-\mathcal{Y}_a$ 与$\mathcal{X}_b-\mathcal{X}_a$ 互素,拥有私钥一方通过连续的两次解密分别得到 $r(\mathcal{Y}_b-\mathcal{Y}_a)$与 $r(\mathcal{X}_b-\mathcal{X}_a)$,然后用欧几里德扩展算法就可以计算出 $r(\mathcal{Y}_b-\mathcal{Y}_a)$与 $r(\mathcal{X}_b-\mathcal{X}_a)$的最大公约数 r,可以求出$\mathcal{Y}_b-\mathcal{Y}_a$ 与$\mathcal{X}_b-\mathcal{X}_a$;
     (3) 拥有私钥一方可以用步骤(2)的结果以及自己的坐标$(\mathcal{X}_a,\mathcal{Y}_a)$计算出另一方的坐标信息$(\mathcal{X}_b,\mathcal{Y}_b)$,造成另一方坐标信息的泄露;
2. 按照该协议计算出的直线斜率虽然在数值方面是正确的,但符号却不一定正确,即该协议未考虑直线斜率的正负问题.这是因为该协议采用的同态加密方案中的加、解密函数都是定义在素域上的函数,加密一个负数实质就是加密其在该素域上的加法逆元,解密结果自然恒为非负数.

过两私有点保密计算一条直线的问题依然是个未彻底解决的公开问题.正如陈志伟等人所阐述的那样,这是对信息安全研究很有价值的安全多方几何计算问题.此外,目前也未见保密计算过两点直线斜率符号协议的报道.

解决过两私有点保密计算一条直线问题的关键是要构造一种既能安全计算过两私有点直线斜率的符号,又能安全计算两私有点坐标差商数值$\left(\frac{|\Delta\mathcal{Y}|}{|\Delta\mathcal{X}|}=\frac{|\mathcal{Y}_b-\mathcal{Y}_a|}{|\mathcal{X}_b-\mathcal{X}_a|}\right)$的方法.也就是说,解决过两私有点保密计算一条直线问题的关键是寻求一种新的方法(不再采用先分别计算出分子 $r(\mathcal{Y}_b-\mathcal{Y}_a)$与分母 $r(\mathcal{X}_b-\mathcal{X}_a)$,然后再通过除法将 $r(\mathcal{Y}_b-\mathcal{Y}_a)$与 $r(\mathcal{X}_b-\mathcal{X}_a)$的共有随机数消除的方法)解决以下两个问题.

1) 能够安全计算出过两私有点直线斜率 k 的符号;

2) 能够安全计算出两私有点坐标差商数值.

解决问题 1)的难点是如何不泄露分子$\mathcal{Y}_b-\mathcal{Y}_a$ 与分母$\mathcal{X}_b-\mathcal{X}_a$ 的符号.因为一旦泄露分子$\mathcal{Y}_b-\mathcal{Y}_a$ 与分母$\mathcal{X}_b-\mathcal{X}_a$ 的符号,就会泄露各方坐标分量的大小关系,进而泄露无解密密钥一方的相对位置信息.解决该问题 2)的难点是如何避免解密方通过解密分离出分子 $r(\mathcal{Y}_b-\mathcal{Y}_a)$与分母 $r(\mathcal{X}_b-\mathcal{X}_a)$.因为一旦解密方分离出 $r(\mathcal{Y}_b-\mathcal{Y}_a)$与 $r(\mathcal{X}_b-\mathcal{X}_a)$,就可以通过除法将 $r(\mathcal{Y}_b-\mathcal{Y}_a)$与 $r(\mathcal{X}_b-\mathcal{X}_a)$的共有随机数消除,进而造成无解密密钥一方私有信息的泄露.为此,本文首先提出了一种可以由加密方选择加密底数的 Paillier[24]变型同态加密方案;然后,基于该同态加密方案构造了一种新的安全两方比较方法,并设计了过两私有点保密计算一条直线协议,还将该协议推广到可归约为保密计算坐标差商的一大类保密几何计算问题中.

本文的创新贡献如下:

- 基于高阶剩余类判定性问题构造了一种新的同态加密方案,并证明了方案在标准模型下是 IND-CPA 安全的;
- 利用新构造的同态加密方案构造了一种新的、安全两方比较大小的方法;
- 基于新构造的同态加密方案设计了一个保密过两个私有点计算一条直线的协议,此协议还包含一个新的安全计算过两私有点直线斜率符号的子协议;
- 计算过两私有点直线斜率的符号时无需调用百万富翁协议,且不造成参与方坐标分量信息(大小)的泄露;
- 将过两私有点保密计算一条直线协议拓展应用到其他涉及保密计算点坐标差商的问题.

1 预备知识

1.1 加密方案的安全性

定义 1. 不可区分安全游戏.

语义安全的概念通常由不可区分性游戏来刻画,这种游戏是由一个系统构建者和一个敌手参与的思维实验.设$\mathcal{E}$为任意一个公钥加密方案,$\mathcal{A}$为任意概率多项式时间的敌手, $Adv_{\mathcal{A},\mathcal{E}}(k)$ 为$\mathcal{A}$在攻击$\mathcal{E}$不可区分游戏中成功的优势,则公钥加密方案的选择明文不可区分(indistinguishability under chosen-plaintext attack,简称 IND-CPA)游戏 $PubK_{\mathcal{A},\mathcal{E}}^{cpa}(k)$ [25]被分定义为:

(1) 输入系统安全参数 1^k,生成密钥对(K_{pub},K_{pri});

(2) $\mathcal{A}$获得公钥 K_{pub},并且它能够访问加密谕言机 $Enc(\cdot)$,经过一些加密问询后输出两个相同长度的明文 m_0 和 m_1;

(3) 系统搭建者随机选择 $b\in\{0,1\}$,然后输出挑战密文 $c=Enc(m_b)$;

(4) $\mathcal{A}$继续调用 $Enc(\cdot)$,输出一个比特位 b'作为对 b 的猜测结果;

(5) 若 $b'=b$,则游戏输出 $PubK_{\mathcal{A},\mathcal{E}}^{cpa}(k)=1$;否则,输出 $PubK_{\mathcal{A},\mathcal{E}}^{cpa}(k)=0$.

如果存在一个可忽略的函数δ,满足:

$$Adv_{A,\mathcal{E}}^{cpa}(k)=\left|\Pr[PubK_{A,\mathcal{E}}^{cpa}(k)=1]-\frac{1}{2}\right|\leqslant\delta(k),$$

则方案$\mathcal{E}$在选择明文攻击下是不可区分加密方案,即,对适应性选择明文攻击是安全的.

1.2 安全多方计算的安全性

- 理想保密计算协议

假设存在绝对可信的第三者(trusted third party,简称 TTP),借助于 TTP,两方安全计算协议可以按照如下方式实施:Alice 与 Bob 分别将各自的输入 a 和 b 告诉 TTP,由 TTP 独立计算 $f(a,b)$,然后将结果分别告诉 Alice 和 Bob.因为 Alice 和 Bob 没有办法从协议中得到除 $f(a,b)$之外的额外信息,这样一个简单的协议是保密程度最高的两方安全计算协议,任何一个计算 $f(a,b)$的实际两方安全计算协议的保密程度都不可能超过这个协议.

- 半诚实参与者

不严格地说,一个半诚实参与者在执行多方安全计算协议的过程中会忠实地履行该协议,但他可能会保留所有中间结果,试图从中间结果推导出结果之外的信息.

设 $f=(f_1,f_2):\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*$是一个概率多项式函数,$\pi$是计算函数 f 的双方协议.协议的输入为 (a,b),执行协议π时 Alice 和 Bob 的 *view* 分别记作 $view_1^{\pi}(a,b)$ 与 $view_2^{\pi}(a,b)$.

$$view_d^{\pi}(a,b)=(a,r_d,m_{d1},m_{d2},...,m_{dk}),$$

其中,$d\in\{1,2\}$,r_d 是 Alice 或 Bob 自己选择的随机数,m_{di} 是 Alice 或 Bob 收到的第 i 个消息;Alice 和 Bob 的输出分别记作 $output_1^{\pi}(a,b)$ 与 $output_2^{\pi}(a,b)$.

定义 2[2]. 对于概率多项式函数 f,如果存在概率多项式时间模拟算法$\mathcal{S}_1$ 与$\mathcal{S}_1$ 使得

$$\{(\mathcal{S}_1(a,f_1(a,b)),f_2(a,b))\}_{a,b}\overset{c}{\equiv}\{(view_1^{\pi}(a,b),output_2^{\pi}(a,b))\}_{a,b} \tag{1(a)}$$

$$\{(f_1(a,b),\mathcal{S}_2(a,f_2(a,b)))\}_{a,b}\overset{c}{\equiv}\{(output_1^{\pi}(a,b),view_2^{\pi}(a,b))\}_{a,b} \tag{1(b)}$$

成立,则称π保密地计算 $f(a,b)$.其中,$\overset{c}{\equiv}$表示计算不可区分.

Goldreich 利用比特承诺和零知识证明理论设计了一种编译器,给该编译器输入在半诚实参与者条件下安全计算 f 的协议π,它可以自动生成在恶意参与者条件下也能安全计算 f 的协议π',π'将迫使恶意的参与者以半诚实方式参与协议的执行,否则就会被发现.很多时候,需要将设计的半诚实参与者条件下的多方安全计算协议π作为编译器的输入,让编译器输出在恶意参与者条件下也能安全计算 f 的协议π'.本文假设协议的参与者都是半诚实的.

- 同态加密方案的安全性对由同态加密方案构造的安全多方计算协议安全性的影响

假设同态加密方案ε对适应性选择明文攻击是安全的,协议Π是由ε构造的安全多方计算协议;假设 Alice 是协议Π的参与方,并假定 Alice 拥有加密系统ε的公、私钥.目前,基本所有以同态加密系统为构造原语设计的安全多方计算协议都隐含规定:协议执行过程中,Alice 不对任何解密问询进行响应,只对最终计算结果的解密进行响应,这与 IND-CPA 安全的要求是一致的.

敌手能够实施更高级别的攻击必须具有如下通信环境:拥有解密密钥一方在通信过程中需要响应其他通信方的解密问询.在使用同态加密系统ε构建的安全多方计算协议中,Alice 不对任何解密问询响应,因此,敌手也就无法实施更高级别的攻击.

对于 Alice 而言,除自己外的其他任何人(包括内部和外部的敌手)只能从 Alice 手里得到密文,不会得到任何密文对应的明文.所以对于 Alice 而言,她用自己的公钥产生的密文对于他人来说是计算不可区分的,这就足以保护自己信息的隐私性.所以,如果用于构造协议Π的加密方案ε对选择明文攻击是安全的,则由ε产生的密文都是计算不可区分的.

对于协议Π的其他参与方而言,则可以利用同态操作在 Alice 私有数据对应密文的基础上做适当的盲化运算,就可以保护自己的隐私数据.

因此,在采用同态加密方案设计的安全多方计算协议中,具有 IND-CPA 安全性的同态加密方案足以保护参与方数据的安全(隐私)性.

1.3 Paillier同态加密方案[24]

Paillier 提出了 3 个加密方案,其中,方案 1(如图 1 所示,图中参数定义如下:p 与 q 为两个等长的大素数,$n=pq$, $\lambda=lcm(p-1,q-1)$, $g=1+kn$ $(k\in Z_n^*)$)具有良好的加法同态性:对多个密文执行乘法运算,可以秘密地实现明文的加运算,即:

$$E(x+y)=E(x)\cdot E(y) \tag{2}$$

加密	明文 $m<n$
	选择一个随机数 $r<n$
	密文 $C=g^m r^n \bmod n^2$
解密	密文 $C<n^2$
	明文 $m=\dfrac{L(C^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$

Fig.1 Paillier's encryption scheme

图 1 Paillier 加密方案

这是一种具有语义安全的加密方案,用这个方案对任意两个等长的明文 m_0 与 m_1 进行加密,m_0 与 m_1 对应的密文 C_0 与 C_1 是计算上不可区分的,即 $C_0 \overset{c}{\equiv} C_1$.

1.4 高阶剩余类判定性问题

定义 3. 高阶剩余类判定性问题(decisional composite residuosity problem,简称 DCR).

简单地讲,高阶剩余类判定性问题就是给定合数 $n=pq$ 和整数 $z\in Z_n^*$,判定 z 是否是模 n^2 的 n 次剩余类,即:判定是否存在 y,使得 $z\equiv y^n \bmod n^2$[24].

用可证安全的形式化语言描述如下.

设 $\boldsymbol{D}$ 是一种区分算法,令 D_{ran} 和 D_ε 是如下两个分布:

$$D_{ran}=\{(n,R)\mid R\xleftarrow{R} Z_{n^2}\} \tag{a}$$

$$D_\varepsilon=\{(n,R)\mid R\leftarrow\{r^n \bmod n^2 \mid r\in Z_n\}\} \tag{b}$$

用 $Adv_{\boldsymbol{D}}(\tau)$表示区分算法 $\boldsymbol{D}$ 能够区分两个分布 D_{ran} 和 D_ε 的优势,其中,τ为系统安全参数.如果给定一个分布 $(n,\boldsymbol{R})\in\{D_{ran},D_\varepsilon\}$,并把区分算法对于分布$(n,\boldsymbol{R})$的输出记作 $\boldsymbol{D}(n,\boldsymbol{R})=D_{ran}$ 或 $\boldsymbol{D}(n,\boldsymbol{R})=D_\varepsilon$,则 $Adv_{\boldsymbol{D}}(\tau)$可以表示成:

$$Adv_{\boldsymbol{D}}(\tau)=|\Pr[\boldsymbol{D}(n,\boldsymbol{R})=D_{ran}]-\Pr[\boldsymbol{D}(n,\boldsymbol{R})=D_\varepsilon]|.$$

DCR 问题是密码学中公认的数学难题[13],所以对于任意多项式时间的概率算法 $\boldsymbol{D}$,存在可忽略的函数$\delta(\tau)$,满足:

$$Adv_{\boldsymbol{D}}(\tau)\leqslant\delta(\tau).$$

如果将上面两个分布 D_{ran} 和 D_ε 中的 $\boldsymbol{R}$ 分别替换成$(\boldsymbol{R}_1,\boldsymbol{R}_2)$和 $(r_1^n \bmod n^2, r_2^n \bmod n^2)$,显然,得到的新分布 D_{ran} 和 D_ε.

$$D_{ran}=\{(n,\boldsymbol{R})=(n,(\boldsymbol{R}_1,\boldsymbol{R}_2))\mid \boldsymbol{R}\xleftarrow{\boldsymbol{R}_1,\boldsymbol{R}_2} Z_{n^2}\} \tag{3(a))}$$

$$D_\varepsilon=\{(n,\boldsymbol{R})=(n,(r_1^n \bmod n^2, r_2^n \bmod n^2))\mid \boldsymbol{R}\leftarrow\{(r_1^n \bmod n^2, r_2^n \bmod n^2)\mid r_1,r_2\in Z_n\}\} \tag{3(b))}$$

仍然满足 $Adv_{\boldsymbol{D}}(\tau)\leqslant\delta(\tau)$.

2 新的同态加密方案及其性能

本文设计了一种新的同态加密方案.该方案同 Paillier 加密方案一样,是用密文的乘运算实现指数上明文的

加同态;但加密用的底数 g 由加密一方依据需要有变化地选择,该方案的构造及性能描述如下.

2.1 Paillier的变体加密方案

该加密方案由密钥生成(Key-Gen)、加密(Enc)和解密(Dec)这 3 个随机算法组成,记作:

$$\mathcal{E}(\textbf{Key-Gen},\textbf{Enc},\textbf{Dec}).$$

- **Key-Gen**:生成两个等长的大素数 p,q,计算:

$$n=pq,\lambda=lcm(p-1,q-1).$$

公钥为 $K_{pub}=(n,1+n)$;私钥为 $K_{pri}=\lambda$;

- **Enc**:加密一方随机选择 $k\in Z_n,r_1\in Z_n,r_2\in Z_n$,对于 $m<n$,计算:

$$g_k=(1+n)^k \bmod n^2, c_1=g_k^m r_1^n \bmod n^2, c_2=g_k r_2^n \bmod n^2;$$

- **Dec**:解密一方执行解密运算:

$$m=\frac{L(c_1^\lambda \bmod n^2)}{L(c_2^\lambda \bmod n^2)} \bmod n, \text{其中}, L(u)=\frac{u-1}{n}, u\in Z_{n^2}^*.$$

证明:

$$\begin{aligned}\frac{L(c_1^\lambda \bmod n^2)}{L(c_2^\lambda \bmod n^2)} \bmod n &= \frac{L(g_k^{\lambda m} \bmod n^2)}{L(g_k^\lambda \bmod n^2)} \bmod n \quad \text{(Carmichael' s theorem)}\\ &= \frac{L((1+n)^{k\lambda m} \bmod n^2)}{L((1+n)^{k\lambda} \bmod n^2)} \bmod n\\ &= \frac{\frac{(1+n)^{k\lambda m} \bmod n^2)-1}{n}}{\frac{(1+n)^{k\lambda} \bmod n^2)-1}{n}} \bmod n\\ &= \frac{(1+n)^{k\lambda m} \bmod n^2)-1}{(1+n)^{k\lambda} \bmod n^2)-1} \bmod n\\ &= \frac{k\lambda mn \bmod n^2}{k\lambda n \bmod n^2} \bmod n\\ &= m.\end{aligned}$$

□

2.2 方案的性能

- 同态性

令 m_1,m_2 是两个明文,用 Paillier 变体方案加密后它们对应的密文分别为

$$Enc(m_1)=(c_1,c_2)=(g_k^{m_1} r_1^n \bmod n^2, c_2=g_k r_2^n \bmod n^2),$$
$$Enc(m_2)=(c_1',c_2')=(g_k^{m_2} (r_1')^n \bmod n^2, c_2=g_k (r_2')^n \bmod n^2).$$

若定义运算:

$$Enc(m_1)\odot Enc(m_2)=(c_1\cdot c_1' \bmod n^2, c_2 \oslash c_2' \bmod n^2),$$

其中,$\oslash$被定义为 $c_2 \oslash c_2' \bmod n^2 = c_2 \text{ or } c_2'$,则:

$$\begin{aligned}Enc(m_1)\odot Enc(m_2) &= (c_1\cdot c_1' \bmod n^2, c_2 \oslash c_2')\\ &= (\{g_k^{m_1} r_1^n \bmod n^2\}\cdot\{g_k^{m_2}(r_1')^n \bmod n^2\} \bmod n^2, \{g_k r_2^n \bmod n^2\} \oslash \{g_k (r_2')^n \bmod n^2\})\\ &= (g_k^{m_1+m_2}(r_1 r_1')^n \bmod n^2, g_k r_2^n \bmod n^2 \text{ or } g_k (r_2')^n \bmod n^2)\\ &= (C_1,C_2)\\ &= (g_k^M R_1^n \bmod n^2, g_k R_2^n \bmod n^2),\end{aligned}$$

其中, $M=m_1+m_2, R_1=r_1 r_1', R_2=r_1 \text{ or } r_1'$.

$$
\begin{aligned}
Dec((C_1,C_2)) &= \frac{L(C_1^{\lambda} \bmod n^2)}{L(C_2^{\lambda} \bmod n^2)} \bmod n \\
&= \frac{L(g_k^{\lambda M} \bmod n^2)}{L(g_k^{\lambda} \bmod n^2)} \bmod n \quad \text{(Carmichael's theorem)} \\
&= \frac{L((1+n)^{k\lambda M} \bmod n^2)}{L((1+n)^{k\lambda} \bmod n^2)} \bmod n \\
&= \frac{\dfrac{(1+n)^{k\lambda M} \bmod n^2)-1}{n}}{\dfrac{(1+n)^{k\lambda} \bmod n^2)-1}{n}} \bmod n \\
&= \frac{(1+n)^{k\lambda M} \bmod n^2)-1}{(1+n)^{k\lambda} \bmod n^2)-1} \bmod n \\
&= \frac{k\lambda Mn \bmod n^2}{k\lambda n \bmod n^2} \bmod n \\
&= M.
\end{aligned}
$$

- 加密底数由加密方选定(解密方不知道).

加密时,底数 g 不再是解密方选定,而是由加密方随机选择,解密方只有同时拥有两个用加密方选择的底数 g 加密的密文才能正确解密.

- 通信双方仅通过 1 次通信就可以传递一个有理数.

加密方向解密方传递有理数 $\mathfrak{R}<n$ 时,加密方按照如下方式计算密文对.

(1) 将有理数 $\mathfrak{R}$ 表示成分数 $\frac{m_1}{m_2}$,其中, $m_1,m_2 \in Z_n^+$;

(2) 随机选择 $k \in Z_n, r_1 \in Z_n, r_2 \in Z_n$,对于 $m_1,m_2<n$,计算:

$$g_k=(1+n)^k \bmod n^2, c_1=g_k^{m_1} r_1^n \bmod n^2, c_2=g_k^{m_2} r_2^n \bmod n^2,$$

并将 (c_1,c_2) 发送给解密方.

收到 (c_1,c_2) 后,解密方通过执行运算:

$$\mathfrak{R}=\frac{L(c_1^{\lambda} \bmod n^2)}{L(c_2^{\lambda} \bmod n^2)},$$

就可以得到有理数 $\mathfrak{R}$(利用此性能可以巧妙地将坐标转化成比值秘密地传递通信对方).

2.3 方案$\mathcal{E}$的安全性

定理 1. 如果 DCR 判定性问题是多项式时间难解的,则方案 $\mathcal{E}$ 在选择明文攻击下具有不可区分安全,即 IND-CPA 安全.

证明:规定 DCR 挑战者的工作方式如下.

1. 运行 **Key-Gen** 算法得到密钥 $(n,1+n)$;
2. 从 Z_n 上随机选取一个不为"0"的数 k,并进行如下计算:

$$g_k=(1+n)^k \bmod n^2;$$

3. 均匀地选取 $d \in \{0,1\}$;
4. 如果 $d=0$,则置 $T=(T_1,T_2)=(r_1^n \bmod n^2, r_2^n \bmod n^2)$;否则,$d=1$ 时,则置 $T=\boldsymbol{R}=(\boldsymbol{R}_1,\boldsymbol{R}_2)$;
5. 将 $(n,1+n,(T_1 g_k^m \bmod n^2, T_2 g_k \bmod n^2),T)$ 发送给攻击者.

设 $\mathcal{E}$(**Key-Gen**,**Enc**,**Dec**)为第 2.1 节描述的加密方案,$\mathcal{A}$ 是一个概率多项式时间敌手,ε 为敌手 $\mathcal{A}$ 在 $PubK_{\mathcal{A},\mathcal{E}}^{cpa}(n)$ 游戏中的获胜优势.可以按照如下方式设计一个解决 DCR 的算法 $\mathcal{B}$.

算法$\mathcal{B}$.

1. 接收 DRSA 挑战者发来的$(n,1+n,(n,\boldsymbol{R}),T)$(敌手并不知道$(n,\boldsymbol{R})$来自 D_{Ran} 与 $D_{\mathcal{E}}$ 中的哪一个分布);
2. 令 $K_{Pub}=(n,1+n)$;
3. 将系统安全参数 1^n 与公钥 K_{Pub} 发给敌手$\mathcal{A}$;
4. 接收来自$\mathcal{A}$的两个等长的消息 m_0 与 m_1;
5. 随机选取 $b\in\{0,1\}$;
6. 设 $c^*=(T_1g_k^m \bmod n^2, T_2g_k \bmod n^2)$ 并将 c^*发送给敌手$\mathcal{A}$;
7. 令 b'为敌手$\mathcal{A}$对 b 的猜测结果;
8. 输出 d'如果 $b=b'$,则令 $d'=0$;如果 $b\neq b'$,则令 $d'=1$).

概率多项式时间算法$\mathcal{B}$赢得 DCR 安全游戏的概率可以用贝叶斯公式求解如下:

$$\left.\begin{aligned}\Pr[d=d'] &= \Pr[d=0]\Pr[d=d'\mid d=0]+\Pr[d=1]\Pr[d=d'\mid d=1]\\ &= \frac{1}{2}\Pr[d'=0\mid d=0]+\frac{1}{2}\Pr[d'=1\mid d=1]\\ &= \frac{1}{2}\Pr[b=b'\mid d=0]+\frac{1}{2}\Pr[b\neq b'\mid d=1]\end{aligned}\right\} \tag{4}$$

若 $d=0$,则 DCR 挑战者置 $T=(T_1,T_2)=(r_1^n \bmod n^2, r_2^n \bmod n^2)$.此时,由于算法$\mathcal{B}$提交给算法$\mathcal{A}$的视图(view)与实际中$\mathcal{A}$攻击$\mathcal{E}$的 $PubK_{\mathcal{B},\mathcal{E}}^{cpa}$ 游戏中的视图是不可区分的,所以在 $d=0$ 时,$b=b'$的概率与敌手$\mathcal{A}$赢得游戏 $PubK_{\mathcal{B},\mathcal{E}}^{cpa}$ 的概率相等,即:

$$\Pr[b=b'\mid d=0]=\frac{1}{2}+\epsilon \tag{5}$$

若 $d=1$,则 DRSA 挑战者置 $T=\boldsymbol{R}=(\boldsymbol{R}_1,\boldsymbol{R}_2)$.因为 $\boldsymbol{R}$ 在 Z_n 上是均匀分布的,所以 $(\boldsymbol{R}_1g_k^m \bmod n^2, \boldsymbol{R}_2g_k \bmod n^2)$ 在 $(Z_{n^2}^*, Z_{n^2}^*)$ 上也是均匀分布的,且独立于 n,m_0,m_1 与 b.又因为随机变量 $n,g_k,\boldsymbol{R}_1g_k^m \bmod n^2, \boldsymbol{R}_2g_k \bmod n^2$ 和 b 是两两相互独立的,因此,公钥 K_{Pub} 和密文 c^*并没有泄露任何关于 b 的信息,从而可得出:b'(由敌手$\mathcal{A}$输出的对 b 的猜测结果)与 b 必定相互独立.又因为 $b=0$ 和 $b=1$ 两个事件发生的概率是均等的,因此有:

$$\Pr[b=b'\mid d=1]=\frac{1}{2} \tag{6}$$

由公式(4)~公式(6)得:

$$\Pr[d=d']=\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\times\frac{1}{2}=\frac{1}{2}+\frac{1}{2}\varepsilon \tag{7}$$

因此,算法$\mathcal{B}$赢得 DCR 安全游戏的优势为

$$|\Pr[d=d']-\Pr[d\neq d']|=\left|\Pr[PubK_{\mathcal{B},\Pi}^{cpa}(n)=1]-\frac{1}{2}\right|=\frac{\varepsilon}{2} \tag{8}$$

由 DCR 假设知,算法$\mathcal{B}$赢得安全游戏 DCR 的优势是可忽略的,所以 $\frac{\varepsilon}{2}$ 是个可忽略值,从而可以推出ε也是可忽略的.因此,敌手$\mathcal{A}$在游戏 $PubK_{\mathcal{A},\mathcal{E}}^{cpa}$ 中,只能以可忽略的优势ε获胜.所以,方案$\mathcal{E}$是 IND-CPA 安全的.

因此,用该方案对任意两个等长的明文 m_0 与 m_1 进行加密,m_0 与 m_1 对应的密文 c_0 与 c_1 是计算上不可区分的,即 $c_0\overset{c}{\equiv}c_1$. □

2.4 加密方案的计算复杂性

1) 理论分析

假定本文方案和 Paillier 方案用到的模数都为 n,并且将一次模乘运算的复杂度 $O(\log^2 n)$设定为算法复杂度衡量的基础单位.因为由二项式展开定理得 $g_k=(1+n)^k \bmod n^2=1+kn$,所以计算 g_k 时,直接可以计算 $1+kn$,而计算

1+kn 的计算复杂度为 $O(\log^2 n)$,所以本文加密算法的复杂度为 $O(\log^3 n+\log^2 n)$,解密算法的复杂度为 $O(\log^3 n)$.而 Paillier 加密、解密算法的计算复杂度均为 $O(\log^3 n)$,显然,本文加密方案的计算复杂性与 Paillier 是同一级别的.

2) 实验验证

实验中用的硬件平台为通用 PC 机,具体资料如下:制造商:Hewlett-Packard Company,型号:p7-1011,处理器:Intel(R) Core(TM) i3-2100 3.10GB,内存:4GB.

实验中用的软件平台如下:64 位 Windows 7(2009 Microsoft Corporation,Service Pack 1),Java Runtime Environment.

将模数 n 取为 512bit 长,选定 k=21,用 Paillier 加密方案和本文加密方案分别对 m=201 在上述实验平台上进行 31 次重复加、解密操作,并将每一次加、解密耗时记录下来,取均值后的结果见表 1 和表 2.

Table 1 Time cost on Paillier's one encryption and one decryption

表 1 Paillier 加密方案中一次加密和一次解密的耗时情况

算法	耗时(ms)
加密	3.612 903 225 8
解密	8.903 225 806 5

Table 2 Time cost on $\mathcal{E}$'s one encryption and one decryption

表 2 加密方案$\mathcal{E}$中一次加密和一次解密的耗时情况

算法	耗时(ms)
加密	6.838 709 677 4
解密	8.93 548 3870 9

解决过两私有点保密计算一条直线问题的实质就是要解决加密方如何向解密方秘密传递两个数 x 与 y 的比值 $\kappa=\frac{y}{x}$(其中, $x,y\in Z_n^+$,并且要求 x 与 y 对解密方保密)的问题.从安全性方面讲,如果采用 ElGamal、DJ[26]和 Paillier 方案实现加密方向解密方保密传递两个数 x 与 y 的比值κ,加密方需要分别加密分子与分母,而且解密方可以由两次独立的解密运算分别得到分子和分母,进而导致 x 与 y 的泄露.而采用我们的方案保密传递两个数 x 与 y 的比值κ,加密方虽然也是分别加密分子与分母,但解密方却不能对两个加密结果分别解密,必须将两个加密结果合在一起才能解密,因而可以避免 x 与 y 信息的泄露.从效率方面讲,在解决秘密传递两个数 x 与 y 的比值 $\kappa=\frac{y}{x}$(其中, $x,y\in Z_n^+$,并且要求 x 与 y 对解密方保密)问题方面,与 Paillier 方案以及 DJ[26]相比,方案ε也是略胜一筹.

方案 DJ[26]是目前所知的效率最高的 Paillier 方案的变体,它的基本运算是模 n^{s+1} 乘运算(其中,n 是 RSA 模,$s\geqslant 1$).它在 s=1 时效率最高,而此时,实质就是 Paillier 方案.下面给出方案$\mathcal{E}$与 Paillier 方案在解决秘密传递两个数 x 与 y 的比值 $\kappa=\frac{y}{x}$(其中, $x,y\in Z_n^+$,并且要求 x 与 y 对解密方保密)问题中开销、安全性方面的一个比较.

3) 在解决秘密传递两个数 x 与 y 的比值κ问题方面,与 Paillier 方案相比,方案$\mathcal{E}$更有优势

加密方有两个整数 $x,y\in Z_n^+$,他在安全协议执行过程中,只想把这两个数的比值κ秘密传递给解密方而不想让解密方得到具体的 x 与 y.

- 采用ε方案秘密传递两个数的比值.

加密方随机选择 $k\in Z_n, r_1\in Z_n, r_2\in Z_n$,对于 $x,y<n$,计算:

$$g_k=(1+k\cdot n)\bmod n^2, c_1=g_k^y r_1^n \bmod n^2, c_2=g_k^x r_2^n \bmod n^2,$$

并将密文(c_1,c_2)发送给解密方.

收到(c_1,c_2)后,解密方通过执行运算:

$$\kappa=\frac{L(c_1^{\lambda} \bmod n^2)}{L(c_2^{\lambda} \bmod n^2)},$$

便得到κ.显然,这个过程只需要花费一次加密和一次解密运算.

因为解密方不知道加密底数 $g_k=(1+k\cdot n) \bmod n^2$,所以他无法像 Paillier 方案那样通过运算:

$$\frac{L(c_1^{\lambda} \bmod n^2)}{L(g_k^{\lambda} \bmod n^2)} \bmod n, \frac{L(c_2^{\lambda} \bmod n^2)}{L(g_k^{\lambda} \bmod n^2)} \bmod n$$

求出 x 与 y.加密方在秘密传递给解密方 x 与 y 的比值(κ)过程中,未造成 x 与 y 的泄露.

- 采用 Paillier 方案秘密传递两个数的比值.

加密方为了不泄露自己的 x 与 y,需要先对 $x,y<n$ 按照如下方式进行盲化.

(1) 随机选择 $r \in Z_n^*$;

(2) 计算:$X=r\cdot x, Y=r\cdot y$.

然后,加密方再随机选择 $r_1 \in Z_n^*, r_2 \in Z_n^*$,对于 $x,y<n$,计算:

$$c_1=g^Y r_1^n \bmod n^2, c_2=g^X r_2^n \bmod n^2,$$

并将密文 c_1 和 c_2 发送给解密方.

收到 c_1 和 c_2 后,解密方通过执行运算:

$$\kappa=\frac{\dfrac{L(c_1^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n}{\dfrac{L(c_2^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n},$$

才可以得到κ.

在此过程中,加密方需要花费 2 次加密运算、2 次解密运算和一次数据盲化.更关键的是,如果 $\gcd(x,y)=1$,则会造成则会造成加密方(即消息发送方)信息的泄露.因为解密方(即消息接收方)可以由两次独立的解密运算:

$$\frac{L(c_1^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n, \frac{L(c_2^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n,$$

分别得到分子和分母的值,然后利用欧几里得扩展算法即可求出消息发送方的 x 与 y,从而造成信息发送方信息的泄露.

由我们的实验数据(见表 1 和表 2)可得:在加密运算耗时方面,方案$\mathcal{E}$几乎是 Paillier 方案的 2 倍;但在解密耗时方面几乎是一样的.表 3 是实现通信双方一次秘密传递κ采用方案$\mathcal{E}$与采用 Paillier 方案关于效率(由加、解密和盲化操作次数体现)和解决问题规模方面的对比.

Table 3 Comparison on operations and their times to privately transmit κ

表 3 一次秘密传递κ需要执行操作、操作次数方面的对比

方法	算法		
	加密	解密	盲化操作
采用 Paillier 加密方案需要执行的次数	2 次	2 次	1 次
采用加密方案$\mathcal{E}$需要执行的次数	1 次(相当于 2 次 Paillier 加密)	1 次(相当于 1 次 Paillier 解密)	0

综上所述可得:在解决秘密传递两个数 x 与 y(其中,$x,y \in Z_n^+$)的比值 $\kappa=\frac{y}{x}$ 问题方面,与以前的 ElGamal、DJ[26]和 Paillier 等同态加密方案相比,方案$\mathcal{E}$更符合设计过两个私有点保密计算直线方程协议的需求.

3 过平面两个私有点保密计算直线方程协议

3.1 问题的形式化描述及解决问题的核心

如图 2 所示,$\boldsymbol{A},\boldsymbol{B}$ 两方分别拥有保密坐标 $A(x_a,y_a),B(x_b,y_b)$,在不泄漏两方私有坐标的情况下,求经过 $\boldsymbol{A},\boldsymbol{B}$ 两方

的直线.

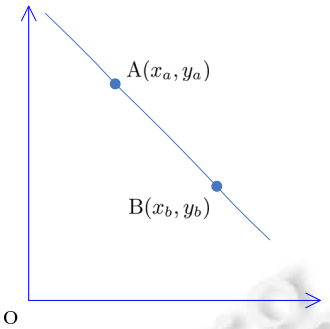


Fig.2 Straight line past ***A*** and ***B***

图 2 过 ***A***,***B*** 两方的直线

设过 ***A***,***B*** 两方私有坐标点直线的斜率为$\mathcal{K}$,则 ***A***,***B*** 两方各自可以用点斜式求得过两方私有坐标点的直线:

$$y=\mathcal{K}(x-x_a)+y_a, y=\mathcal{K}(x-x_b)+y_b, \text{其中, } \mathcal{K}=\frac{y_b-y_a}{x_b-x_a}.$$

解决该问题的关键是:如何保密地求出过 ***A***,***B*** 两方私有坐标点直线的斜率$\mathcal{K}$,却又不泄露 ***A***,***B*** 两方私有坐标点信息.

3.2 过平面两个私有点保密计算直线方程的协议

Step 1. 保密计算过两私有点直线斜率的符号.

- ***A*** 方先运行方案$\mathcal{E}$(**Key-Gen**,**Enc**,**Dec**)的密钥生成算法产生公私钥:公钥(n,1+n),私钥λ;然后,按照如下方式加密自己的坐标信息:

$$c_{x_a}=(1+n)^{x_a} r_{sx_a}^n \bmod n^2 \tag{9(a)}$$

$$c_{y_a}=(1+n)^{y_a} r_{sy_a}^n \bmod n^2 \tag{9(b)}$$

并将 (c_{x_a}, c_{y_a}) 发送给 ***B*** 方;

- ***B*** 方收到 (c_{x_a}, c_{y_a}) 后按照如下方式工作.

(1) 随机选择 4 个不等的随机数 $k_{sx1}, k_{sy1}, r_{sx}, r_{sy} \in Z_n$,利用方案$\mathcal{E}$(**Key-Gen**,**Enc**,**Dec**)加密及其同态性计算:

$$c_{(r_{sx}+x_a)}=((c_{x_a})^{k_{sx1}} \bmod n^2)\times(1+k_{sx1}n)^{r_{sx}} r_{sx1}^n \bmod n^2 \tag{10(a)}$$

$$c_{(r_{sx}+x_b)}=(1+k_{sx1}n)^{(r_{sx}+x_b)} r_{sx2}^n \bmod n^2 \tag{10(b)}$$

$$c_{(r_{sy}+y_a)}=((c_{y_a})^{k_{sy1}} \bmod n^2)\times(1+k_{sy1}n)^{r_{sy}} r_{sy1}^n \bmod n^2 \tag{11(a)}$$

$$c_{(r_{sy}+y_b)}=(1+k_{sy1}n)^{(r_{sy}+y_b)} r_{sy2}^n \bmod n^2 \tag{11(b)}$$

(2) 随机选择ℓ_1-2(其中,$\frac{\ell_1}{2}$ 为奇数)个随机数对 $(r_1,r_1'),(r_2,r_2'),\ldots,(r_{\ell_1-2},r_{\ell_1-2}') \in Z_n$,满足 $\frac{r_1}{r_1'},\frac{r_2}{r_2'},\ldots,\frac{r_{\ell_1-2}}{r_{\ell_1-2}'}$ ($2\leqslant h\leqslant \ell_1-2$)中大于 1 和小于 1 的个数相等且为偶数,即都为 $\frac{\ell_1}{2}-1$;

(3) 随机选取ℓ_1-2 个$\kappa_i \in Z_n$,其中,$1\leqslant i\leqslant \ell_1-2$,计算 $g_i=1+\kappa_i n$;

(4) 对于指标 i 指示的$\ell-2$ 对 (r_i,r_i'),计算:

$$c_{r_i}=(g_i)^{r_i} r_{r_i}^n \bmod n^2 \tag{12(a)}$$

$$c_{r_i'}=(g_i)^{r_i'} r_{r_i'}^n \bmod n^2 \tag{12(b)}$$

而得到$\ell-2$ 个密文对;

(5) 对 ℓ_1 个密文对 $(c_{(r_{sx}+x_a)},c_{(r_{sx}+x_b)}),(c_{(r_{sy}+y_a)},c_{(r_{sy}+y_b)}),(c_{r_1},c_{r_1'}),(c_{r_2},c_{r_2'}),...,(c_{r_{\ell-2}},c_{r_{\ell-2}'})$ (或 $(c_{(r_{sx}+x_b)},c_{(r_{sx}+x_a)})$, $(c_{(r_{sy}+y_b)},c_{(r_{sy}+y_a)}),(c_{r_1},c_{r_1'}),(c_{r_2},c_{r_2'}),...,(c_{r_{\ell-2}},c_{r_{\ell-2}'})$)做随机置换,记置换后的密文对为:

$$(c_{s1},c_{s2}),(c_{s3},c_{s4}),...,(c_{s(2\ell_1-1)},c_{s(2\ell_1)}),$$

并发给 ***A***;

- ***A*** 收到$(c_{si},c_{s(i+1)})$后计算:

$$\partial=\prod_{i=1}^{\ell_1}P\left(\frac{L(c_{si}^{\lambda})}{L(c_{s(i+1)}^{\lambda})}\right) \tag{13}$$

其中,函数 $P(X)$的定义如下:

$$P(X)=\begin{cases}+1, & X>1\\ -1, & X<1\end{cases}.$$

Step 2. ***A*** 方随机选择 $r_{x_a}\neq r_{sx_a},r_{y_a}\neq r_{sy_a}$,然后用自己的公钥将自己的坐标信息按照如下方式重新加密.

$$c_{x_a}=(1+n)^{x_a}r_{x_a}^n \bmod n^2 \tag{14(a)}$$

$$c_{y_a}=(1+n)^{y_a}r_{y_a}^n \bmod n^2 \tag{14(b)}$$

并将 (c_{x_a},c_{y_a}) 发送给 ***B*** 方;

Step 3. ***B*** 方收到 (c_{x_a},c_{y_a}) 后按照如下方式工作.

① 随机选择两个不等的随机数 k_{x1},k_{y1},并计算 $(c_{x_a})^{k_{x1}} \bmod n^2,(c_{y_a})^{k_{y1}} \bmod n^2$;

② 利用 Paillier 变体方案加密自己的坐标信息:

$$c_{x_b}=(1+k_{x1}n)^{-x_b}r_{x_b}^n \bmod n^2 \tag{15(a)}$$

$$c_{y_b}=(1+k_{y1}n)^{-y_b}r_{y_b}^n \bmod n^2 \tag{15(b)}$$

其中,$r_{x_b},r_{y_b}\in Z_n$;

③ 计算 $k_{x1}\Delta x=k_{x1}(x_a-x_b)$与 $k_{y1}\Delta y=k_{y1}(y_a-y_b)$的密文:

$$c_{k_{x1}\Delta x}=c_{x_a}\cdot c_{x_b} \bmod n^2 \tag{16(a)}$$

$$c_{k_{y1}\Delta y}=c_{y_a}\cdot c_{y_b} \bmod n^2 \tag{16(b)}$$

④ 随机选择 $2\ell_2$(ℓ_2 为偶数,并且对 ***A*** 是保密的)个数 $k_{x2},k_{x3},...,k_{x(\ell_2+1)}\in Z_n,k_{y2},k_{y3},...,k_{y(\ell_2+1)}\in Z_n$,按照步骤①~步骤③的方式计算$\ell_2$ 个密文对 $(c_{k_{xj}\Delta x},c_{k_{yj}\Delta y})$,其中,$2\leqslant j\leqslant \ell_2+1$;

⑤ 随机选择 $2(\ell-\ell_2-1)$个数 $k_{x(\ell_2+2)},k_{x(\ell_2+3)},...,k_{x\ell}\in Z_n,k_{y(\ell_2+2)},k_{y(\ell_2+3)},...,k_{y\ell}\in Z_n$;

⑥ 随机选取$(\ell-\ell_2-1)$个$\kappa_i\in Z_n$,其中,$\ell_2+2\leqslant i\leqslant \ell$,计算 $g_i=1+\kappa_i n$;

⑦ 对于指标 i 指示的$(\ell-\ell_2-1)$对 k_{xi},k_{yi} 计算:

$$c_{k_{xi}}=(g_i)^{k_{xi}}r_{k_{xi}}^n \bmod n^2 \tag{17(a)}$$

$$c_{k_{yi}}=(g_i)^{k_{yi}}r_{k_{yi}}^n \bmod n^2 \tag{17(b)}$$

得到$(\ell-\ell_2-1)$对密文,其中,步骤①~步骤⑦步中的 $k_{x1},k_{x2},...,k_{x\ell}$ 与 $k_{y1},k_{y2},...,k_{y\ell}$ 满足:

$$k_{x1}\cdot k_{x2}\cdot ....\cdot k_{x\ell}=k_{y1}\cdot k_{y2}\cdot ....\cdot k_{y\ell};$$

⑧ 将第④步中得到的ℓ_2 个密文对中 $\frac{\ell_2}{2}$ 个置成 $(c_{k_{xj}\Delta x},c_{k_{yj}\Delta y})$,另外的 $\frac{\ell_2}{2}$ 个置成 $(c_{k_{xj}\Delta y},c_{k_{xj}\Delta x})$,然后将这$\ell_2$ 个密文对与步骤③中得到的 1 个密文对以及步骤⑦中得到的$(\ell-\ell_2-1)$个密文对进行置换,得到$(c_{y1},c_{x1}),(c_{y2},c_{x2}),\ldots,(c_{y\ell},c_{\ell})$.并按此顺序发给 ***A***.

Step 4. ***A*** 收到 $(c_{y1},c_{x1}),(c_{y2},c_{x2}),...,(c_{y\ell},c_{\ell})$ 后,按照如下方式计算斜率.

$$\mathcal{K}=\frac{L(c_{y1}^{\lambda} \bmod n^2)}{L(c_{x1}^{\lambda} \bmod n^2)}\times\frac{L(c_{y2}^{\lambda} \bmod n^2)}{L(c_{x2}^{\lambda} \bmod n^2)}\times\ldots\times\frac{L(c_{y\ell}^{\lambda} \bmod n^2)}{L(c_{x\ell}^{\lambda} \bmod n^2)}\times\partial \tag{18}$$

计算直线 L_{AB}:

$$y=\mathcal{K}(x-x_a)+y_a,$$

并将$\mathcal{K}$发送给 ***B***;

Step 5. ***B*** 收到$\mathcal{K}$后计算直线 L_{AB}:

$$y=\mathcal{K}(x-x_b)+y_b.$$

3.3 正确性分析

定理. 在过平面两个私有点保密计算一条直线方程的协议中,安全斜率符号计算进程能正确计算出斜率符号.

证明:证明过程省略了系统初始化部分,因为通过函数:

$$P(X)=\begin{cases}+1, & X>1\\ -1, & X<1\end{cases},$$

其值可以判定 $X>1$ 还是 $X<1$.

如果 $\frac{x}{y}>1$,则 $\frac{x}{y}>\frac{x+m}{y+m}>1$;如果 $\frac{x}{y}<1$,则 $\frac{x}{y}<\frac{x+m}{y+m}<1$.

所以有 $P\left(\frac{x_a}{x_b}\right)=P\left(\frac{x_a+m}{x_b+m}\right)$ 和 $P\left(\frac{y_a}{y_b}\right)=P\left(\frac{y_a+m}{y_b+m}\right)(m>0)$ 成立.

如果置 $P'(X'-Y')=\begin{cases}+1, & X'>Y'\\ -1, & X'<Y'\end{cases}$,则有:

$$P\left(\frac{x_a}{x_b}\right)=P'(x_a-x_b)或\left(P\left(\frac{x_b}{x_a}\right)=P'(x_b-x_a)\right).$$

同理有 $P\left(\frac{y_a}{y_b}\right)=P'(y_a-y_b)或\left(P\left(\frac{y_b}{y_a}\right)=P'(y_b-y_a)\right)$.

因此,等式(13): $\partial=\prod_{i=1}^{\ell_1}P\left(\frac{L(c_{si}^{\lambda})}{L(c_{s(i+1)}^{\lambda})}\right)$ 能正确求出直线斜率的符号;并且在计算此符号的过程中,***A***,***B*** 两方中任何一方的秘密信息都没有被泄漏. □

定理 3. 过平面两个私有点保密做直线方程的协议能正确求出经过两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***,***B*** 位置坐标的密文信息分别为

$$Enc(\boldsymbol{A}(x_a,y_a))=((1+n)^{x_a}r_{x_a}^n \bmod n^2,(1+n)^{y_a}r_{y_a}^n \bmod n^2) \tag{19(a)}$$

$$Enc(\boldsymbol{B}(x_b,y_b))=((1+k_{x1}n)^{x_b}r_{x_b}^n \bmod n^2,(1+k_{y1}n)^{y_b}r_{y_b}^n \bmod n^2) \tag{19(b)}$$

$$\begin{aligned}Enc(\boldsymbol{A}(x_a^{k_{x1}},y_a^{k_{y1}}))&=((1+n)^{k_{x1}x_a}r_{x_a}^{k_{x1}n} \bmod n^2,(1+n)^{k_{y1}y_a}r_{y_a}^{k_{y1}n} \bmod n^2)\\&=((1+k_{x1}n)^{x_a}r_{x_a}^{k_{x1}n} \bmod n^2,(1+k_{y1}n)^{y_a}r_{y_a}^{k_{y1}n} \bmod n^2)\end{aligned} \tag{20}$$

B 由密文信息 (c_{x_a},c_{y_a}) 计算 $Enc(k_{x1}\Delta x),Enc(k_{y1}\Delta y)$:

$$c_{k_{x1}\Delta x}=c_{x_b}\cdot((c_{x_a})^{k_{x1}} \bmod n^2) \bmod n^2=(1+k_{x1}n)^{x_a-x_b}((r_{x_b})^{n-x_b}r_{x_a}^{k_{x1}})^n \bmod n^2 \tag{21(a)}$$

$$c_{k_{y1}\Delta y}=c_{y_b}\cdot((c_{y_a})^{k_{y1}} \bmod n^2) \bmod n^2=(1+k_{y1}n)^{y_a-y_b}((r_{y_b})^{n-y_b}r_{y_a}^{k_{y1}})^n \bmod n^2 \tag{21(b)}$$

将第 3.2 节 Step 3 第④步中得到的ℓ_2个密文对中的 $\frac{\ell_2}{2}$ 个置成 $(c_{k_{xj}\Delta x},c_{k_{xj}\Delta y})$,另外的 $\frac{\ell_2}{2}$ 个置成 $(c_{k_{yj}\Delta y},c_{k_{xj}\Delta x})$,然后将这$\ell_2$个密文对与其他$\ell-\ell_2$个密文对随机置换成:

$$(c_{y1},c_{x1}),(c_{y2},c_{x2}),...,(c_{y\ell},c_{\ell});$$

接收到 $(c_{y1},c_{x1}),(c_{y2},c_{x2}),...,(c_{y\ell},c_{\ell})$,$\boldsymbol{A}$ 进行计算:

$$\left.\begin{aligned}
&\frac{L(c_{y1}^{\lambda} \bmod n^2)}{L(c_{x1}^{\lambda} \bmod n^2)} \times \frac{L(c_{y2}^{\lambda} \bmod n^2)}{L(c_{x2}^{\lambda} \bmod n^2)} \times ... \times \frac{L(c_{y\ell}^{\lambda} \bmod n^2)}{L(c_{x\ell}^{\lambda} \bmod n^2)} \times \partial = \\
&\partial \times \frac{L(c_{y1}^{\lambda} \bmod n^2) \cdot L(c_{y2}^{\lambda} \bmod n^2) \cdot ... \cdot L(c_{y\ell}^{\lambda} \bmod n^2)}{L(c_{x1}^{\lambda} \bmod n^2) \cdot L(c_{x2}^{\lambda} \bmod n^2) \cdot ... \cdot L(c_{x\ell}^{\lambda} \bmod n^2)} = \\
&\partial \times \frac{k_{y1} \cdot k_{y2} \cdot ... \cdot k_{y(\ell_2+1)} (\Delta y)^{\frac{\ell_2}{2}+1} \cdot (\Delta x)^{\frac{\ell_2}{2}} \cdot \kappa_1 k_{y(\ell_2+2)} \cdot \kappa_2 k_{y(\ell_2+3)} \cdot ... \cdot \kappa_{\ell-\ell_2-1} k_{y\ell}}{k_{x1} \cdot k_{x2} \cdot ... \cdot k_{x(\ell_2+1)} (\Delta x)^{\frac{\ell_2}{2}+1} \cdot (\Delta y)^{\frac{\ell_2}{2}} \cdot \kappa_1 k_{x(\ell_2+2)} \cdot \kappa_2 k_{x(\ell_2+3)} \cdot ... \cdot \kappa_{\ell-\ell_2-1} k_{x\ell}} (\text{commutative law of multiplication}) = \\
&\frac{\Delta y}{\Delta x}(k_{x1} \cdot k_{x2} \cdot ... \cdot k_{x\ell} = k_{y1} \cdot k_{y2} \cdot ... \cdot k_{y\ell}) = \mathcal{K}
\end{aligned}\right\} \quad (22)$$

$\mathcal{K}$即为过 $\boldsymbol{A}$,$\boldsymbol{B}$ 两方坐标点直线的斜率.$\boldsymbol{A}$ 根据直线的点斜式表示方式可求得直线:

$$y=\mathcal{K}(x-x_a)+y_a.$$

将$\mathcal{K}$发送给 $\boldsymbol{B}$ 后,$\boldsymbol{B}$ 同样可以用点斜式求得直线:

$$y=\mathcal{K}(x-x_b)+y_b.$$

在此个过程中,$\boldsymbol{A}$ 发给 $\boldsymbol{B}$ 的信息都是密文的形式,$\boldsymbol{B}$ 没有私钥无法获知有关 $\boldsymbol{A}$ 的坐标信息;$\boldsymbol{A}$ 方不知道ℓ_2,因而无法通过求解方程 $(\Delta y)^{\frac{\ell_2}{2}+1} \cdot (\Delta x)^{\frac{\ell_2}{2}} = a$ 与方程 $(\Delta y)^{\frac{\ell_2}{2}} \cdot (\Delta x)^{\frac{\ell_2+1}{2}} = b$ (a,b 都是已知的)计算 $\boldsymbol{B}$ 方的坐标信息.因此,$\boldsymbol{A}$,$\boldsymbol{B}$ 任何一方的秘密信息都没有被泄漏,且完成了过两点直线方程的求解,正确性得证. □

4 安全性分析

安全多方计算协议中有两种通信模型,即信息论模型和密码学模型.在信息论模型下,任意两个参与者之间的信息都是通过一条安全信道传递的,攻击者具有无限的计算能力;在密码学模型中,攻击者可以看到所有通信者之间传递的信息,但它不能改动通信者之间传递的信息,且它的攻击能力是概率多项式时间的.因本文设计的协议中,参与者之间是在密码学模型下传递信息的,所以本文主要从密码学安全的角度去分析协议的安全性.

定理 4. 在半诚实模型下,过平面两个私有点保密计算一直线方程的协议是安全的.

证明:显然,安全求解直线斜率符号的过程与安全求解斜率$\mathcal{K}$的过程是相同且相互独立的,因此,两个过程的安全证明也是相似的.为简洁起见,以下只给出安全求解斜率$\mathcal{K}$的模拟证明过程.因为安全求解直线斜率符号的过程中用到的随机数与安全求解斜率$\mathcal{K}$的过程中用到的随机数是相互独立的,所以在下面的模拟范例中,可将斜率符号∂视作 $\boldsymbol{A}$ 的一个随机输入.

由于协议的关键在于保密计算过两点的斜率,所以在证明协议的安全性时,我们将斜率作为输出构造预备知识里的符合第 2.2 节中公式(1(a))和公式(1(b))的模拟器;$\boldsymbol{A}$ 输入位置坐标的密文信息为 (c_{x_a},c_{y_a}),$\boldsymbol{B}$ 输入位置坐标的密文信息为 (c_{x_b},c_{y_b}).

$\boldsymbol{A}$ 在执行协议Π的过程中,视图(view)记为

$$\begin{aligned}
View_A^{\Pi}(\boldsymbol{A},\boldsymbol{B}) = View_A^{\Pi}(\boldsymbol{A},K_{pub},K_{pri},c_{x_a},c_{y_a},\partial,\mathcal{K},\boldsymbol{B},k_{x1},k_{y1},(c_{x_a})^{k_{x1}} \bmod n^2,(c_{y_a})^{k_{y1}} \bmod n^2,(k_{x2},...,k_{x\ell}),\\
(k_{y2},...,k_{y\ell}),(g_2,...,g_{\ell}),c_{x_b},c_{y_b},(c_{k_{y1}\Delta y},c_{k_{y2}},...,c_{k_{y\ell}}),(c_{k_{x1}\Delta x},c_{k_{x2}},...,c_{k_{x\ell}})).
\end{aligned}$$

输出记为

$$\begin{aligned}
&Output_A^{\Pi}(\boldsymbol{A},\boldsymbol{B})(\boldsymbol{A},K_{pub},K_{pri},c_{x_a},c_{y_a},\partial,\mathcal{K},\boldsymbol{B},(k_{x1},...,k_{x\ell}),(k_{y1},...,k_{y\ell}),(c_{x_a})^{k_{x1}} \bmod n^2,\\
&(c_{y_a})^{k_{y1}} \bmod n^2,(g_2,...,g_{\ell}),c_{x_b},c_{y_b},(c_{k_{y1}\Delta y},c_{k_{y2}},...,c_{k_{y\ell}}),(c_{k_{x1}\Delta x},c_{k_{x2}},...,c_{k_{x\ell}})) = \mathcal{K}.
\end{aligned}$$

下面构造模拟器 $\boldsymbol{S}_1$ 模拟 $\boldsymbol{A}$ 方协议的执行过程.

模拟器 $\boldsymbol{S}_1$ 的输入为

$$\boldsymbol{S}_1(\boldsymbol{A},f_1(\boldsymbol{A},\boldsymbol{B}),f_2(\boldsymbol{A},\boldsymbol{B}))=\{\boldsymbol{A},K_{pub},K_{pri},c_{x_a},c_{y_a},\partial,\mathcal{K},f_1(\boldsymbol{A},K_{pub},c_{x_a},c_{y_a},\partial),\boldsymbol{B},C_y,C_x,f_2(K_{pri},C_x,C_y),\mathcal{K}\},$$

其中, $f_2(K_{pri},C_x,C_y,\mathcal{K})=\mathcal{K},C_y=(c_{y1},c_{y2},...,c_{y\ell}),C_x=(c_{x1},c_{x2},...,c_{x\ell})$.

$\boldsymbol{S}_1$ 利用系统公钥加密坐标(x_a,y_a),得到密文 c_{x_a} 与 c_{y_a} .C_y 与 C_x 分别存在一个分量满足:

$$c'_{y_a}=c_{y_b}\cdot(c_{yi})^{\frac{1}{k_{y1}}} \tag{23}$$

$$c'_{x_a}=c_{x_b}\cdot(c_{xi})^{\frac{1}{k_{x1}}} \tag{24}$$

由于 Paillier 变体加密方案在 n 次剩余困难假设下是语义安全的,所以 $C_y=(c_{y1},c_{y2},...,c_{y\ell})$ 的各分量间是计算不可区分的.同理, $C_x=(c_{x1},c_{x2},...,c_{x\ell})$ 的各分量间是也是计算不可区分的.进而可得:

$$c'_{y_a}\overset{c}{\equiv}c_{yi},c'_{x_a}\overset{c}{\equiv}c_{xi},$$

其中,$1\leqslant i\leqslant\ell$即 $(c'_{y_a},c_{y1},c_{y2},...,c_{y\ell})$ 与 $(c'_{x_a},c_{x1},c_{x2},...,c_{x\ell})$ 是两个各自分量间满足多项式电路计算不可区分的元组.$\boldsymbol{S}_1$ 利用系统私钥,按照算式(15)计算斜率$\mathcal{K}$.

令 $\boldsymbol{S}_1(\boldsymbol{A},f_1(\boldsymbol{A},\boldsymbol{B}))=(\boldsymbol{A},K_{pub},K_{pri},c_{x_a},c_{y_a},\partial,\mathcal{K},\boldsymbol{B},(k_{x1},...,k_{x(\ell+2)}),(k_{y1},...,k_{y(\ell+2)}),C_y,C_x)$,则模拟器为

$$\boldsymbol{S}_1(\boldsymbol{A},f_1(\boldsymbol{A},\boldsymbol{B}),f_2(\boldsymbol{A},\boldsymbol{B}))=(\boldsymbol{A},K_{pub},K_{pri},c_{x_a},c_{y_a},\partial,\mathcal{K},\boldsymbol{B},(k_{x1},...,k_{x(\ell+2)}),(k_{y1},...,k_{y(\ell+2)}),C_y,C_x)=\mathcal{K},$$

而 A 的真实视图:

$$\{View_A^{\Pi}(\boldsymbol{A},\boldsymbol{B}),Output_A^{\Pi}(\boldsymbol{A},\boldsymbol{B})\}=(\boldsymbol{A},K_{pub},K_{pri},c_{x_a},c_{y_a},\partial,\mathcal{K},\boldsymbol{B},(k_{x1},...,k_{x(\ell+2)}),(k_{y1},...,k_{y(\ell+2)}),C_y,C_x).$$

因此,可以构造一个满足:

$$\{\boldsymbol{S}_1(\boldsymbol{A},f_1(\boldsymbol{A},\boldsymbol{B}),f_2(\boldsymbol{A},\boldsymbol{B})\}\overset{c}{\equiv}\{View_A^{\Pi}(\boldsymbol{A},\boldsymbol{B}),Output_B^{\Pi}(\boldsymbol{A},\boldsymbol{B})\} \tag{25}$$

的模拟器 $\boldsymbol{S}_1$,其中, $Output_B^{\Pi}(\boldsymbol{A},\boldsymbol{B})$ 完全由 $View_A^{\Pi}(\boldsymbol{A},\boldsymbol{B})$ 决定.

类似地,也可以构造一个满足:

$$\{f_1(\boldsymbol{A},\boldsymbol{B}),\boldsymbol{S}_2(\boldsymbol{A},f_2(\boldsymbol{A},\boldsymbol{B})\}\overset{c}{\equiv}\{Output_A^{\Pi}(\boldsymbol{A},\boldsymbol{B}),View_B^{\Pi}(\boldsymbol{A},\boldsymbol{B})\} \tag{26}$$

的模拟器 $\boldsymbol{S}_2$,其中 $Output_A^{\Pi}(\boldsymbol{A},\boldsymbol{B})$ 完全由 $View_B^{\Pi}(\boldsymbol{A},\boldsymbol{B})$ 决定.故定理 4 成立. □

5 解决保密过两点计算一条直线协议的推广

解决此问题的关键在于如何保密地求出两私有点坐标的差商.因此,只要是能够归约为保密地求两私有点坐标差商的一类问题,都可以应用该协议解决.如安全两方线段求交点问题.

Alice 和 Bob 分别拥有一条直线 l_A:$y=a_Ax+b_A,x\in[m_A,n_A]$与 l_B:$y=a_Bx+b_B,x\in[m_B,n_B]$(其中,$m_A,n_A,m_B,n_B\in Z_n$),他们想保密地计算两条线段的交点,即:二者协同计算完毕后,彼此都无法获得除了交点外的任何信息.

其他可以用类似方法解决的问题还有:判断同一平面 3 个私有点是否共线问题、两方保密求叉积问题、判定同一平面两个私有多边形是否相交等问题的解决,最终是要归约为保密地求两私有点坐标差商问题.下面以安全两方线段求交点问题为例,讨论归约为保密地求两私有点坐标差商的一类问题的应用.

对于同一平面中的两条线段,位置关系关系有如图 3 所示的 5 种情形.

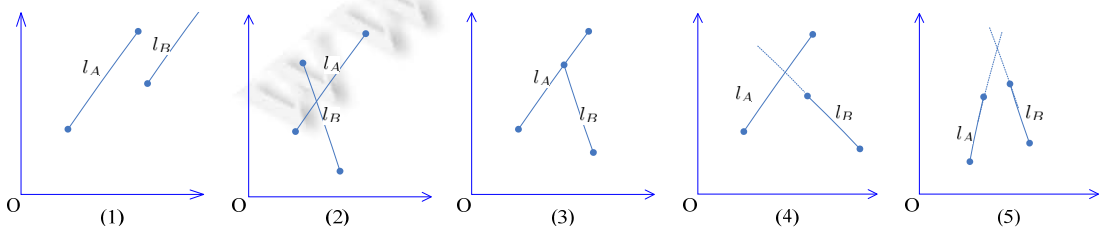


Fig.3 Location relationships of two line segments

图 3 两线段的位置关系

不失一般性,在此,我们只考虑图3中的情形(2).在这种情形下,安全两方线段求交点问题实质是保密求解满足条件(式(27))的方程组(式(28))的解(式(29))的问题.

$$m_A \leqslant x \leqslant n_A, m_B \leqslant x \leqslant n_B \tag{27}$$

$$\begin{cases} y = a_A x + b_A \\ y = a_B x + b_B \end{cases} \tag{28}$$

$$\begin{cases} x = \dfrac{b_B - b_A}{a_B - a_A} \\ y = a_A x + b_A \text{ or } y = a_B x + b_B \end{cases} \tag{29}$$

而安全计算方程解的问题又归约为保密求解两私有点坐标差商的问题,因此,调用第 4.2 节中的过两点保密计算一条直线的协议,按照如下方式就可以保密地求出两方线段求交点:

$$\frac{b_B - b_A}{a_B - a_A}, y = a_A x + b_A 或 y = a_B x + b_B.$$

解决方法如下.

Step 1. 确定两线段交点横坐标的符号.

- Alice 先运行方案$\mathcal{E}$(**Key-Gen**,**Enc**,**Dec**)的密钥生成算法产生公私钥:公钥(n,1+n),私钥λ;然后,按照如下方式加密自己线段所在直线表达式的参数:

$$c_{a_A} = (1+n)^{a_A} r_{sa_A}^n \bmod n^2 \tag{30(a)}$$

$$c_{b_A} = (1+n)^{b_A} r_{sb_A}^n \bmod n^2 \tag{30(b)}$$

  并将 (c_{x_a}, c_{y_a}) 发送给 Bob;

- Bob 收到 (c_{x_a}, c_{y_a}) 后,按照如下方式工作.

  (1) 随机选择 4 个不等的随机数 $k_{sx1}, k_{sy1}, r_{sx}, r_{sy} \in Z_n$,利用方案$\mathcal{E}$(**Key-Gen**,**Enc**,**Dec**)加密及其同态性计算:

$$c_{(r_{sx}+a_A)} = ((c_{a_A})^{k_{sx1}} \bmod n^2) \times (1+k_{sx1}n)^{r_{sx}} r_{sx1}^n \bmod n^2 \tag{31(a)}$$

$$c_{(r_{sx}+a_B)} = (1+k_{sx1}n)^{(r_{sx}+a_B)} r_{sx2}^n \bmod n^2 \tag{31(b)}$$

$$c_{(r_{sy}+b_A)} = ((c_{b_A})^{k_{sy1}} \bmod n^2) \times (1+k_{sy1}n)^{r_{sy}} r_{sy1}^n \bmod n^2 \tag{32(a)}$$

$$c_{(r_{sy}+b_B)} = (1+k_{sy1}n)^{(r_{sy}+b_B)} r_{sy2}^n \bmod n^2 \tag{32(b)}$$

  (2) 随机选择ℓ_1-2(其中,$\dfrac{\ell_1}{2}$ 为奇数)个随机数对 $(r_1, r_1'), (r_2, r_2'), ..., (r_{\ell_1-2}, r_{\ell_1-2}') \in Z_n$,满足 $\dfrac{r_1}{r_1'}, \dfrac{r_2}{r_2'}, ..., \dfrac{r_{\ell_1-2}}{r_{\ell_1-2}'}$ ($2 \leqslant h \leqslant \ell_1-2$)中大于 1 和小于 1 的个数相等且为偶数,即,都为 $\dfrac{\ell_1}{2}-1$;

  (3) 随机选取ℓ_1-2 个$\kappa_i \in Z_n$,其中,$1 \leqslant i \leqslant \ell_1-2$,计算 $g_i=1+\kappa_i n$;

  (4) 对于指标 i 指示的$\ell-2$ 对 (r_i, r_i'),计算:

$$c_{r_i} = (g_i)^{r_i} r_{r_i}^n \bmod n^2 \tag{33(a)}$$

$$c_{r_i'} = (g_i)^{r_i'} r_{r_i'}^n \bmod n^2 \tag{33(b)}$$

  而得到ℓ_1-2 个密文对;

  (5) 将ℓ_1 个密文对 $(c_{(r_{sx}+a_A)}, c_{(r_{sx}+a_B)}), (c_{(r_{sy}+b_A)}, c_{(r_{sy}+b_B)}), (c_{r_1}, c_{r_1'}), (c_{r_2}, c_{r_2'}), ..., (c_{r_{\ell-2}}, c_{r_{\ell-2}'})$ (或 $(c_{(r_{sx}+a_B)}, c_{(r_{sx}+a_A)})$, $(c_{(r_{sy}+b_B)}, c_{(r_{sy}+b_A)}), (c_{r_1}, c_{r_1'}), (c_{r_2}, c_{r_2'}), ..., (c_{r_{\ell-2}}, c_{r_{\ell-2}'})$)做随机置换,得 $(c_{s1}, c_{s2}), (c_{s3}, c_{s4}), ..., (c_{s(2\ell_1-1)}, c_{s(2\ell_1)})$,并发给 Alice;

- Alice 收到 $(c_{s1}, c_{s2}), (c_{s3}, c_{s4}), ..., (c_{s(2\ell_1-1)}, c_{s(2\ell_1)})$ 后,计算:

$$\partial=\prod_{i=1}^{\ell_1}P\left(\frac{L(c_{si)}^{\lambda})}{L(c_{s(i+1)}^{\lambda})}\right) \tag{34}$$

Step 2. Bob 继续按照如下方式工作.

① 随机选择两个不等的随机数 k_{x1},k_{y1},并计算 $(c_{a_A})^{k_{x1}} \bmod n^2,(c_{b_A})^{k_{y1}} \bmod n^2$;

② 利用 Paillier 变体方案加密自己私有线段所在直线表达是的参数:

$$c_{a_B}=(1+k_{x1}n)^{-a_B}r_{x_b}^n \bmod n^2 \tag{35(a)}$$

$$c_{b_B}=(1+k_{y1}n)^{-b_B}r_{y_b}^n \bmod n^2 \tag{35(b)}$$

其中,$r_{x_b},r_{y_b}\in Z_n$;

③ 计算 $k_{x1}\Delta x=k_{x1}(x_a-x_b)$与 $k_{y1}\Delta y=k_{y1}(y_a-y_b)$的密文.

$$c_{k_{x1}\Delta x}=c_{a_A}\cdot c_{a_B} \bmod n^2 \tag{36(a)}$$

$$c_{k_{y1}\Delta y}=c_{b_A}\cdot c_{b_B} \bmod n^2 \tag{36(b)}$$

④ 随机选择 $2\ell_2(\ell_2$ 为偶数,并且对 Alice 是保密的)个数 $k_{x2},k_{x3},...,k_{x(\ell_2+1)}\in Z_n,k_{y2},k_{y3},...,k_{y(\ell_2+1)}\in Z_n$,按照步骤①~步骤③的方式计算 ℓ_2 个密文对 $(c_{k_{xj}\Delta x},c_{k_{yj}\Delta y})$,其中,$2\leqslant j\leqslant \ell_2+1$;

⑤ 随机选择 $2(\ell-\ell_2-1)$个数 $k_{x(\ell_2+2)},k_{x(\ell_2+3)},...,k_{x\ell}\in Z_n,k_{y(\ell_2+2)},k_{y(\ell_2+3)},...,k_{y\ell}\in Z_n$;

⑥ 随机选取 $\ell-\ell_2-1$ 个 $\kappa_i\in Z_n$,其中,$\ell_2+2\leqslant i\leqslant \ell$,计算 $g_i=1+\kappa_i n$;

⑦ 对于指标 i 指示的 $\ell-\ell_2-1$ 对 k_{xi},k_{yi},计算:

$$c_{k_{xi}}=(g_i)^{k_{xi}}r_{k_{xi}}^n \bmod n^2 \tag{37(a)}$$

$$c_{k_{yi}}=(g_i)^{k_{yi}}r_{k_{yi}}^n \bmod n^2 \tag{37(b)}$$

得到 $\ell-\ell_2-1$ 对密文,其中,步骤①~步骤⑦中的 $k_{x1},k_{x2},...,k_{x\ell}$ 与 $k_{y1},k_{y2},...,k_{y\ell}$ 满足:

$$k_{x1}\cdot k_{x2}\cdot ....\cdot k_{x\ell}=k_{y1}\cdot k_{y2}\cdot ....\cdot k_{y\ell};$$

⑧ 将第④步中得到的 ℓ_2 个密文对中的 $\frac{\ell_2}{2}$ 个置成 $(c_{k_{xj}\Delta x},c_{k_{yj}\Delta y})$,另外的 $\frac{\ell_2}{2}$ 个置成 $(c_{k_{yj}\Delta y},c_{k_{xj}\Delta x})$,然后将这 ℓ_2 个密文对与步骤③中得到的 1 个密文对以及步骤⑦中得到的 $\ell-\ell_2-1$ 个密文对做随机置换,得到(c_{y1},c_{x1}),(c_{y2},c_{x2}),…, $(c_{y\ell},c_{\ell})$,并按此顺序发给 Alice.

Step 3. Alice 收到 $(c_{y1},c_{x1}),(c_{y2},c_{x2}),...,(c_{y\ell},c_{\ell})$ 后,按照如下方式计算交点的横坐标.

$$x=\frac{L(c_{y1}^{\lambda} \bmod n^2)}{L(c_{x1}^{\lambda} \bmod n^2)}\times\frac{L(c_{y2}^{\lambda} \bmod n^2)}{L(c_{x2}^{\lambda} \bmod n^2)}\times...\times\frac{L(c_{y\ell}^{\lambda} \bmod n^2)}{L(c_{x\ell}^{\lambda} \bmod n^2)}\times\partial \tag{38}$$

并将 x 发送给 Bob;如果 $m_A\leqslant x\leqslant n_A$,则将 x 代入直线方程直线 l_A:$y=a_Ax+b_A$ 计算出 y;

Step 4. Bob 收到 x 后,如果 $m_B\leqslant x\leqslant n_B$,则将 x 代入直线方程直线 l_B:$y=a_Bx+b_B$ 计算出 y.

6 效率分析

计算复杂度方面:执行此协议需要执行 $2(\ell_1+\ell)$次加密、$\ell_1+\ell$次解密操作.如果以一次自模乘运算的复杂度 $O(\log^2 n)$作为衡量算法复杂度的基础单位,则本协议的计算复杂度为 $O((\ell_1+\ell)\log^3 n)$.而这个值相对基于 Paillier 加密方案设计的百万富翁协议的计算复杂度(依据文献[16]的结果:基于 Paillier 加密方案设计的百万富翁协议的计算复杂度为 $O(n\log^3 n)$)要小得多.由于在本文协议中,安全求解斜率符号和安全求解斜率这两个进程可并行执行,所以当安全求解斜率符号和安全求解斜率这两个进程并行执行时,本文协议的计算复杂度可降到 $O((\ell_1+\ell)\log^3 n)$.显然,这是一个很大提升.

通信复杂度方面:Alice 和 Bob 在执行此协议过程中无需调用百万富翁协议,仅需要通信 $\ell_1+\ell+4$ 次.

7 结束语

本文首先提出了一个Paillier变体同态加密方案,并证明了其在标准模型下是IND-CPA安全的.用此方案可以高效地解决过两个私有点保密地计算一条直线、保密地求两条线段的交点等可归约为保密求坐标差商的一类问题.

References:

[1] Yao AC. Protocols for secure computations. In: Proc. of the 23rd Annual Symp. on Foundations of Computer Science (SFCS 2008). Washington: IEEE Computer Society Press, 1982. 160−164. [doi: 10.1109/SFCS.1982.38]

[2] Goldreich O. Foundations of Cryptography: Vol.2, Basic Applications. Cambridge University Press, 2004. 615−626.

[3] Naor M, Pinkas B. Oblivious transfer and polynomial evaluation. In: Proc. of the 31st Annual ACM Symp. on Theory of Computing. Berlin, Heidelberg: Springer-Verlag, 1999. 245−254. [doi: 10.1145/301250.301312]

[4] Yao A. How to generate and exchange secrets. In: Proc. of the 27th Annual Symp. on Foundations of Computer Science. Washington: IEEE Computer Society Press, 1986. 162−167. [doi: 10.1109/SFCS.1986.25]

[5] Lindell Y, Pinkas B. Secure two-party computation via cut-and-choose oblivious transfer. Journal of Cryptology, 2012,25(4): 680−722. [doi: 10.1007/s00145-011-9107-0]

[6] Asharov G, Lindell Y, Schneider T, Zohner M. More efficient oblivious transfer and extensions for faster secure computation. In: Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications Security. Berlin, Heidelberg: Springer-Verlag, 2013. 535−548.

[7] Liu ML, Xiao LL, Zhang ZF. A type of secret sharing scheme based random walks on graphs. Science in China: Series E, 2007, 37(1):199−208 (in Chinese with English abstract). http://scholar.google.com/scholar?cluster=15401696449733775O3&hl=zh-CN&as_sdt=0,5 [doi: 10.3321/j.issn:1006-9275.2007.02.008]

[8] Cramer R, Damgård I, Maurer U. General secure multi-party computation from any linear secret-sharing scheme. In: Proc. of the Advances in Cryptology—EUROCRYPT 2000. Berlin, Heidelberg: Springer-Verlag, 2000. 316−334. [doi: 10.1007/3-540-45539-6_22]

[9] Cramer R, Damgård I, Nielsen JB. Multiparty computation from threshold homomorphic encryption. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2001. 280−299. [doi: 10.1007/3-540-44987-6_18]

[10] Damgård I, Pastro V, Smart N, Zakarias S. Multiparty computation from somewhat homomorphic encryption. In: Proc. of the Advances in Cryptology—CRYPTO 2012. Berlin, Heidelberg: Springer-Verlag, 2012. 643−662. [doi: 10.1007/978-3-642-32009-5_38]

[11] Boneh D, Goh EJ, Nissim K. Evaluating 2-DNF formulas on ciphertexts. In: Proc. of the Theory of Cryptography Conf. Berlin, Heidelberg: Springer-Verlag, 2005. 325−341. [doi: 10.1007/978-3-540-30576-7_18]

[12] Lin HY, Tzeng WG. An efficient solution to the millionaires' problem based on homomorphic encryption. In: Proc. of the Applied Cryptography and Network Security. Berlin, Heidelberg: Springer-Verlag, 2005. 456−466. [doi: 10.1007/11496137_31]

[13] López-Alt A, Tromer E, Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proc. of the 44th Annual ACM Symp. on Theory of Computing. New York: ACM, 2012. 1219−1234.

[14] Lagendijk R L, Erkin Z, Barni M. Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation. Signal Processing Magazine, IEEE, 2013,30(1):82−105.

[15] Li SD, Wang DS. Efficient secure multiparty computation based on homomorphic encryption. Chinese Journal of Electronics, 2013, 41(4):798−803 (in Chinese with English abstract). http://www.ejournal.org.cn/EN/article/downloadArticleFile.do?attachType=PDF&id=7759 [doi: 10.3969/j.issn.0372-2112.2013.04.029]

[16] Chen ZW, Zhang JM, Li ZC. Design for secure two-party computation protocol based on ElGamal variant's homomorphic. Journal on Communication, 2015,36(2):204−211 (in Chinese with English abstract). http://www.cnki.com.cn/Article/CJFDTotal-TXXB201502023 [doi: 10.11959/j.issn.1000-436x.2015050]

[17] Du W, Atallah MJ. Secure multi-party computation problems and their applications: a review and open problems. In: Proc. of the 2001 Workshop on New Security Paradigms. Berlin, Heidelberg: Springer-Verlag, 2001. 13−22. [doi: 10.1145/508171.508174]

[18] Luo YL, Huang LS, Xu WJ, Jing WW. A protocol for privacy-preserving intersect-determination of two polygons. Chinese Journal of Electronics, 2007,35(4):685−691 (in Chinese with English abstract). [doi: 10.3321/j.issn:0372-2112.2007.04.016]

[19] Wang Q, Luo Y, Huang L. Privacy-Preserving protocols for finding the convex hulls. In: Proc. of the 3rd Int'l Conf. on Availability, Reliability and Security (ARES 2008). Berlin, Heidelberg: Springer-Verlag, 2008. 727−732. [doi: 10.1109/ARES.2008.11]

[20] Zhang F, Sun XD, Chang HY, Zhao GS. Research on privacy-preserving two-party collaborative filtering recommendation. Acta Electronica Sinica, 2009,37(1):84−89(in Chinese with English abstract). [doi: 10.3321/j.issn:0372-2112.2009.01.015]

[21] Sun MH, Luo SS, Xin Y, Yang YX. Secure two-party line segments intersection scheme and its application in privacy-preserving convex hull intersection. Journal of China Institute of Communications, 2013,34(1):30−42 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-436x.2013.01.004]

[22] Chen L, Lin B. Privacy-Preserving point-inclusion two-party computation protocol. In: Proc. of the 2013 5th Int'l Conf. on Computational and Information Sciences (ICCIS). Berlin, Heidelberg: Springer-Verlag, 2013. 257−260. [doi: 10.1109/ICCIS.2013.75]

[23] Shundong L, Chunying W, Daoshun W, Dai YQ. Secure multiparty computation of solid geometric problems and their applications. Information Sciences, 2014,282:401−413. [doi: 10.1016/j.ins.2014.04.004]

[24] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes. In: Proc. of the Advances in Cryptology—EUROCRYPT'99. Berlin, Heidelberg: Springer-Verlag, 1999: 223-238.

[25] Katz J, Lindell Y. Introduction to Modern Cryptography. Boca Raton: CRC Press, 2014.

[26] Damgård I, Jurik M. A generalisation, a simplication and some applications of paillier's probabilistic public-key system. In: Proc. of the Int'l Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2001. 119−136.

附中文参考文献:

[7] 刘木兰,肖亮亮,张志芳.类基于图上随机游动的密钥共享体制.中国科学:信息科学(中文版),2007,37(1):199−208. http://scholar.google.com/scholar?cluster=15401696449733775O3&hl=zh-CN&as_sdt=0,5 [doi: 10.3321/j.issn:1006-9275.2007.02.008]

[15] 李顺东,王道顺.基于同态加密的高效多方保密计算.电子学报,2013,41(4):798−803. http://www.ejournal.org.cn/EN/article/downloadArticleFile.do?attachType=PDF&id=7759 [doi: 10.3969/j.issn.0372-2112.2013.04.029]

[16] 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.通信学报,2015,36(2):204−211. http://www.cnki.com.cn/Article/CJFDTotal-TXXB201502023 [doi: 10.11959/j.issn.1000-436x.2015050]

[18] 罗永龙,黄刘生,徐维江,荆巍巍.一个保护私有信息的多边形相交判定协议.电子学报,2007,35(4):685−691. [doi: 10.3321/j.issn:0372-2112.2007.04.016]

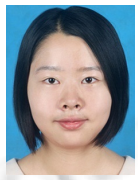
[20] 张锋, 孙雪冬, 常会友, 赵淦森. 两方参与的隐私保护协同过滤推荐研究. 电子学报, 2009,37(1):84−89. [doi: 10.3321/j.issn:0372-2112.2009.01.015]

[21] 孙茂华,罗守山,辛阳,杨义先.安全两方线段求交协议及其在保护隐私凸包交集中的应用.通信学报,2013,34(1):30−42. [doi: 10.3969/j.issn.1000-436x.2013.01.004]

巩林明(1979－),男,山东胶州人,博士,讲师,主要研究领域为密码学,信息安全.

李顺东(1963－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.

窦家维(1963－),女,博士,副教授,主要研究领域为密码学,信息安全.



郭奕旻(1992－),女,博士生,主要研究领域为信息安全,密码学.

王道顺(1963－),男,博士,副教授,博士生导师,主要研究领域为视觉密码,秘密共享.