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

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

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

输出记为

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

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.

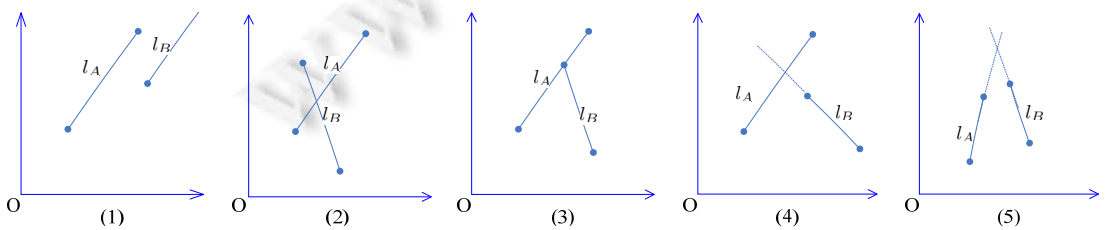


Fig.3 Location relationships of two line segments

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]

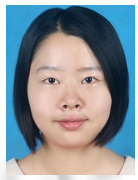
[20] 张锋, 孙雪冬, 常会友, 赵淦森. 两方参与的隐私保护协同过滤推荐研究. 电子学报, 2009,37(1):84−89. [doi: 10.3321/j.issn:0372-2112.2009.01.015]

[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.