$r_i^{\chi_1} r_j^{\chi_2}$ 不能被 n 整除,从而可得 $r_x \neq 0$),其中,$\gamma \in Z_{n-1}$ 之间的整数.

因为 $R_i = r_i^n (\text{mod } n^2)(1 \leqslant i \leqslant k), R_j = r_j^n (\text{mod } n^2)(1 \leqslant j \leqslant k)$,所以,

$$\begin{aligned} R_x &= R_i^{\chi_1} \cdot R_j^{\chi_2} (\text{mod } n^2) \\ &= (r_i^n)^{\chi_1} \cdot (r_j^n)^{\chi_2} (\text{mod } n^2) \\ &= (r_i^{\chi_1} r_j^{\chi_2})^n (\text{mod } n^2) \\ &= (r_x + \gamma n)^n (\text{mod } n^2) \\ &= \sum_{k=0}^{n} \binom{n}{k} r_x^{n-k} (\gamma n)^k (\text{mod } n^2) \\ &= r_x^n (\text{mod } n^2). \end{aligned}$$

(2) 加密运算采用计算 $R_x = R_i^{\chi_1} \cdot R_j^{\chi_2} \mod n^2$ 的方式引入随机变量,在语义安全层面不会削弱方案的安全性.

R 虽然是公开的,但 $R_1, R_2, ..., R_\ell \in R$,$\ell$以及 $\chi_1, \chi_2, ..., \chi_\ell \in \{0, ..., \ell\}$ 都是加密者在加密运算中随机选择的,因此,以 $R_1, R_2, ..., R_\ell \in R$ 为随机种子,由随机函数 $R_x = R_1^{\chi_1} \cdot R_2^{\chi_2} \cdot ... \cdot R_\ell^{\chi_\ell} \mod n^2 = r_x^n \mod n^2$ 计算得到的 R_x 与计算 $(1+kn)^0 \cdot r_{x'}^n \mod n^2$ (其中,$r_{x'} \in Z_n^*$ 是随机选择的)是等效的,因此,任何敌手由 R 计算 R_x 的困难性与破解 Paillier 加密方案的困难性是等价的.

综上所述,加密方案$\mathcal{E}$将计算 $R_i = r_i^n (\text{mod } n^2)(1 \leqslant i \leqslant k, r_i \in Z_n^*)$ 委托给云服务器执行,在语义安全的安全层面上是合理的.

2.2.2 替换运算的正确性

定理 1. $1+m\cdot(g-1)(\text{mod } n^2)$的结果与模指数运算 $g^m \text{ mod } n^2$ 的结果是等价的,即

$$1+m\cdot(g-1)(\text{mod } n^2) \Leftrightarrow g^m \text{ mod } n^2.$$

证明:因为 $g=1+kn\ (k \in Z_n^+)$,所以,

$$1+m\cdot(g-1)(\text{mod } n^2)=1+m\cdot(1+kn-1)(\text{mod } n^2)=1+m\cdot kn(\text{mod } n^2);$$

又由二项式展开定理得:

$$g^m \mod n^2 = (1+kn)^m \mod n^2 = \sum_{\kappa=0}^{m} \binom{m}{\kappa} 1_x^{m-\kappa} (kn)^\kappa \mod n^2 = 1 + \binom{m}{1} \cdot kn \mod n^2 = 1 + m \cdot kn \mod n^2.$$

综上可得:$1+m\cdot(g-1)(\text{mod } n^2) \Leftrightarrow g^m \text{ mod } n^2$. □

2.2.3 解密正确性

因为

$$\begin{aligned} c &= ((1+m\cdot(g-1))(\text{mod } n^2)) \cdot ((R_i \cdot R_j \mod n^2) \mod n^2) \mod n^2 \\ &= (1+m\cdot(1+kn-1)(\text{mod } n^2)) \cdot (r_x^n \mod n^2) \mod n^2 \\ &= ((1+kn)^m \mod n^2) \cdot (r_x^n \mod n^2) \mod n^2 \\ &= g^m r_x^n \mod n^2, \end{aligned}$$

所以有:

$$\frac{L(c^\lambda \mod n^2)}{L((1+\lambda\cdot(g-1)) \mod n^2)} \mod n = \frac{(c^\lambda \mod n^2)-1}{((1+\lambda\cdot kn) \mod n^2)-1} \mod n = \frac{(1+m\cdot kn)-1}{(1+kn)-1} \mod n = m.$$

2.3 安全性分析

定理 2. 如果 DCR 是难解问题,则$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)具有第 1.1 节中定义 1 所定义的不可区分安全性.

证明:在此先回忆一下 DCR 问题挑战者的工作方式.

- 在安全时间 1^k 内,通过执行算法$\mathcal{G}(1^k)$算法产生两个大素数 p 和 q,以及它们的乘积 n.
- 在 Z_n 上随机选取一个数 r,并从{0,1}中均匀选取一个数 f.

- 若 f 为 0,则将$\mathcal{R}$置为 $r^n \bmod n^2$;若 f 为 1,则将$\mathcal{R}$置成 R.

设$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)是 **2.1** 节中构造的方案,将攻击$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)时,敌手使用的多项式时间算法记作$\mathcal{A}$,下面利用算法$\mathcal{A}$构造一个算法$\mathcal{B}$,用于解决 DCR 问题.该算法的具体工作方式如下.

(1) 接收 DCR 挑战者发来的(n,(n,$\mathcal{R}$));

(2) 令 pk=(n,1+kn);

(3) 将 1^n 和 pk 发送给$\mathcal{A}$;

(4) 接收$\mathcal{A}$发来的消息 m_0 和 m_1;

(5) 均匀地选取 $d\in\{0,1\}$;

(6) 令 $C^*=(n,y,y,y',y'',(g')^{m_d}\cdot\mathcal{R}(\bmod n^2))$, 并将 C^*发送给$\mathcal{A}$;

(7) 用 d'表示敌手$\mathcal{A}$对 d 的猜测结果;

(8) 输出 f'(如果 d=d',则置 f'=0;如果 $d\neq d'$,则置 f'=1).

因为算法$\mathcal{B}$只通过调用算法$\mathcal{A}$实现且只调用了 3 次,而作为构成算法$\mathcal{B}$的子算法$\mathcal{A}$是在多项式时间内可被完成的算法,所以通过 3 次调用算法$\mathcal{A}$而实现的算法$\mathcal{B}$是一种在多项式时间内可被完成的算法.因此,$\mathcal{G}(1^k)$也是一种在多项式时间内完成的算法.于是,构造算法$\mathcal{B}$在 DCR 安全游戏中获胜的概率可以表示成贝叶斯公式形式:

$$\left.\begin{aligned}\Pr[f=f']&=\Pr[f=0]\Pr[f=f'\mid f=0]+\Pr[f=1]\Pr[f=f'\mid f=1]\\&=\frac{1}{2}\Pr[f'=0\mid f=0]+\frac{1}{2}\Pr[f'=1\mid f=1]\\&=\frac{1}{2}\Pr[d=d'\mid f=0]+\frac{1}{2}\Pr[d\neq d'\mid f=1]\end{aligned}\right\}\tag{3}$$

当 f=0 时,DCR 挑战者置$\mathcal{R}$=$r^n \bmod n^2$.这样,由算法$\mathcal{A}$构造的算法$\mathcal{B}$呈现给掌握算法$\mathcal{A}$的敌手的视图与掌握算法$\mathcal{A}$的敌手在实际攻击$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)的安全游戏中获取的视图相同.因此,掌握算法$\mathcal{A}$的敌手在攻击$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)的安全游戏中获胜的概率等于 d=d'在条件 f=0 下的条件概率,即

$$\Pr[d=d'\mid f=0]=\frac{1}{2}+\delta\tag{4}$$

当 f=1 时,DCR 挑战者将$\mathcal{R}$置成 R.因为 $R\in Z_{n^2}$ 是均匀选取的,所以,执行运算 $(g')^{m_d}\cdot\mathcal{R}(\bmod n^2)$ 后的结果在群 Z/n^2Z 上是均匀分布的;又因为 3 个随机变量 m_0,m_1,d 相互独立,因此,pk 和 C^*没有暴露关于 d 的任何消息,这意味着掌握算法$\mathcal{A}$的敌手对于 d 的猜测结果 d'与 d 相互独立.若在{0,1}上随机选取 d,则 d=0 或 d=1 的概率各为 $\frac{1}{2}$,故有:

$$\Pr[d=d'\mid f=1]=\frac{1}{2}\tag{5}$$

成立.联立公式(3)~公式(5),我们可以得到:

$$\Pr[f=f']=\frac{1}{2}\left(\frac{1}{2}+\delta\right)+\frac{1}{2}\times\frac{1}{2}=\frac{1}{2}+\frac{1}{2}\delta\tag{6}$$

因此,算法$\mathcal{B}$在 DCR 安全游戏中获胜的优势为

$$\left|\Pr[f=f']-\frac{1}{2}\right|=\left|\left(\frac{1}{2}+\frac{1}{2}\delta\right)-\frac{1}{2}\right|=\frac{\delta}{2}\tag{7}$$

由第 1.1 节中定义 1 可知,在 DCR 安全性游戏中,利用算法$\mathcal{A}$构造的算法$\mathcal{B}$获胜的优势是一个可忽略的量,所以 $\frac{\delta}{2}$ 是一个可忽略的值.这意味δ也是一个可忽略的量.所以利用算法$\mathcal{A}$的敌手在攻击方案$\mathcal{E}$的 IND-CPA 安全游戏中获胜的优势是一个可忽略的量,即$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)具有 IND-CPA 安全性. □

2.4 加密方案的效率分析

因为同态加密方案$\mathcal{E}$中的计算 $R_i=r_i^n \bmod n^2$ 是在预处理阶段由云服务器完成,并且加密者可以在加密前的预处理阶段从云服务器下载集合 $R=\{R_i \mid R_i=r_i^n \bmod n^2\}$, 加密时利用集合中的元素通过执行简单的几次模乘运算($R_x=R_i^{\chi_1}\cdot R_j^{\chi_2} \bmod n^2$, 其中,$(\chi_1,\chi_2\in\{0,\ldots,\ell\})\wedge(\chi_1+\chi_2\geqslant 2)$)即可秘密地得到 $r_x^n \bmod n^2$, 无需再做 n 次复杂的自模乘运算.同时,加密时运算复杂度高的模指数运算 $g^m \bmod n^2$(解密时 $g^\lambda \bmod n^2$)是用与之运算结果等价的、运算简单高效的模乘运算 $1+m\cdot(g-1)(\bmod n^2)$(解密时 $1+\lambda\cdot(g-1)(\bmod n^2)$)替代实现的;若忽略预处理时间,则用方案$\mathcal{E}$加密一个消息的总计需要花费 $6+\lambda$次模乘运算.而用 Paillier 方案加密一个小小的总开销绝不会少于 $2n$ 次模乘运算.表 1 是加密方案$\mathcal{E}$和 Paillier 方案在加、解密效率方面的对比.

Table 1 Comparative analysis on the efficiency of encryption and decryption

表 1 加、解密效率对比分析

类型	加密开销(自模乘运算($r_x^2 \bmod n^2$)次数)	解密开销(自模乘运算($r_x^2 \bmod n^2$)次数)	总计
Paillier 方案	不少于 n	不少于 n	不少于 $2n$
方案$\mathcal{E}$	–	$2+\lambda$	$4+\lambda$

3 保密社交意愿探测协议

3.1 保密社交意愿应用背景描述及其形式化

Alice(需求者)是保险公司的职员,某天在某一个城市推销保险产品,她只想约谈现在正好在某个区域内的客户(可能住在该区域,也可能正在该区域且有空闲时间),她与不想向不在该区域且不愿约谈的用户透露自己的活动区域,例如她想约谈客户 Bob,但 Bob 只想让 Alice 知道他是否可被约谈而不想透露自己的具体位置.Bob 和 Alice 怎样做才能同时实现他们的各自的目的呢?然而,安全多方几何计算为解决这种问题提供了一种可行的方法.我们将 Bob 和 Alice 采用安全多方几何计算思路实现保密测试社交意愿的问题称为保密社交意愿探测问题,其形式化描述如下:

Alice 拥有一个有 K 个顶点 $p_{a_1},p_{a_2},\ldots,p_{a_K}$ ($p_i=(a_{x_i},a_{y_i})$,$1\leqslant i\leqslant K$) 构成的私有凸多边形 P,表示她现在利益最大的活动范围.其中,该多边形的边是按逆时针方向标注的,如图 2 所示(以 K=7 为例).

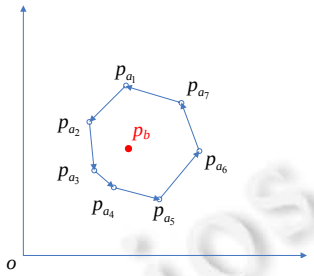


Fig.2 Abstract geometrical figure of private social-willing testing

图 2 保密社交意愿探测几何抽象图

Bob 拥有一个私有点 $p_b=(b_x,b_y)$,表示他现在所处的位置.Alice 想知道 Bob 是否处在自己的想活动的范围内,Bob 不想透露自己的具体位置.我们设计一个这样的安全多方计算协议要实现对 Alice 与 Bob 的隐私保护.

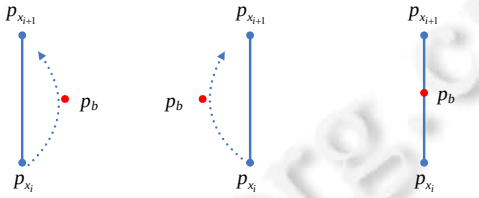
- 协议结束时,Alice 只得到一个意愿探测的结果(一个布尔值),而 Bob 的具体位置信息对于 Alice 仍然是一个秘密.
- 协议结束时,最多只得到 Alice 多边形的边数 $K-1$(Bob 没有得到意愿探测的结果),而 Alice 的活动区域的形状、位置与活动区域的大小对于 Bob 仍然是一个秘密.

3.2 保密社交意愿探测协议

3.2.1 判定凸多边形与一个点位置关系

非保密的近感探测问题实际上就是判定某个凸多边形 P(有 K 个顶点 $p_{a_1},p_{a_2},...,p_{a_K}$)是否包含一个点 p_b=(b_x,b_y)的问题.可以通过 K 次计算有向线段 $\overrightarrow{p_ip_{i+1}}$ 与点 p_b=(b_x,b_y)的位置关系来实现[24−26,29].对于点 p_i,p_b,p_{i+1} 构成的有序元组⟨p_i,p_b,p_{i+1}⟩在平面上可能对应着 3 种位置关系(如图 3 所示).

- 正向:3 个点构成的方向角∠p_i,p_b,p_{i+1} 为逆时针走向(如图 3(a)所示).
- 反向:3 个点构成的方向角∠p_i,p_b,p_{i+1} 为顺时针走向(如图 3(b)所示).
- 零向:3 个点构成的方向角∠p_i,p_b,p_{i+1}=180°,即 p_i,p_b,p_{i+1} 共线(如图 3(c)所示).



(a) 正向 (b) 反向 (c) 零向

Fig.3 Position relations between a point and a line segment

图 3 点与线段的位置关系

假设点 p_i,p_b,p_{i+1} 的坐标分别为 $p_i=(a_{x_i},a_{y_i}),p_b=(b_x,b_y),p_{i+1}=(a_{x_{i+1}},a_{y_{i+1}})$,则 3 点构成的方向角∠$p_i$,$p_b$,$p_{i+1}$ 的方向可以通过计算下列行列式来确立:

$$\left.\begin{aligned}D_i&=\begin{vmatrix}a_{x_i}-b_x & a_{y_i}-b_y\\ a_{x_{i+1}}-b_x & a_{y_{i+1}}-b_y\end{vmatrix}\\&=b_x(a_{y_{i+1}}-a_{y_i})+b_y(a_{x_i}-a_{x_{i+1}})+(a_{y_i}a_{x_{i+1}}-a_{x_i}a_{y_{i+1}})\\&=b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}}-(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})\end{aligned}\right\}\tag{8}$$

其中,D_i>0,D_i<0,D_i=0 分别对应着图 3(a)~图 3(c).

因此,下面的算法可以正确计算出近感探测的结果.

凸多边形与点的关系判定算法.

输入:由 K 个按逆时针顺序访问的顶点 $p_{a_1},p_{a_2},...,p_{a_K}$ 构成的凸多边形 P,点 p_b.

输出:“1”,如果 p_b 在 P 内;“0”,否则 p_b 不在 P 内.

(1) 对于 i∈{1,2,…,K−1}计算点 p_b 与有向线段 $\overrightarrow{p_ip_{i+1}}$ 两个端点所构成的方向角∠p_i,p_b,p_{i+1} 的方向 D_i.

(2) 如果对于∀i∈{1,2,…,K−1}都有 D_i≤0,则返回“1”;否则,返回“0”.

3.2.2 保密社交意愿探测协议

利用上述凸多边形与点的位置关系判定方法、第 2.1 节中设计的带云辅助计算的同态加密方案以及一种新的保密符号计算方法,设计了一个保密社交意愿探测协议.

保密社交意愿探测协议.

输入:Alice 输入由 K 个按逆时针顺序访问的顶点 $p_{a_1},p_{a_2},...,p_{a_K}$ 构成的凸多边形 P,Bob 输入点 p_b.

输出:“1”,如果 p_b 在 P 内;“0”,否则 p_b 不在 P 内.

1. COR:云服务器随机选 $r_1,r_2,...,r_k\in Z_n^*$(其中,k≤n),计算足够多的 $R_i=r_i^n(\mathrm{mod}\ n^2)(1\leqslant i\leqslant k)$,并将它们存储在集合 R 中.当加密者或者是数据运算者需要 $r_x^n(\mathrm{mod}\ n^2)$ 时,随时可以从该服务器上下载 R,利用集合 R 中的某些元素通过一些简单的模乘运算就可以秘密地得到 $r_x^n(\mathrm{mod}\ n^2)$.

2. Alice 运行加密系统$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)的密钥生成算法 Kgen,生成公钥 K_{pub}=(n,1+kn)和私钥 K_{pri}=λ;

3. Alice 首先从云服务器上下载集合 R 并随机选取 $R_{A_{j1}},R_{A_{j2}},...,R_{A_{j12}}\in R$,然后按照如下方式操作:

(1) 对于 $j\in\{1,2,\ldots,K-1\}$计算(假设 Alice 将χ_1,χ_2取作$\chi_1=\chi_2=1$,并置$\ell=2$):

$$E_\varepsilon(a_{y_{j+1}})\equiv(1+a_{y_{j+1}}(g-1))\cdot R_{A_{j1}}\cdot R_{A_{j2}} \bmod n^2,\ E_\varepsilon(a_{x_j})\equiv(1+a_{x_j}(g-1))\cdot R_{A_{j3}}\cdot R_{A_{j4}} \bmod n^2,$$

$$E_\varepsilon(a_{y_j}a_{x_{j+1}})\equiv(1+a_{y_j}a_{x_{j+1}}(g-1))\cdot R_{A_{j5}}\cdot R_{A_{j6}} \bmod n^2,\ E_\varepsilon(a_{y_j})\equiv(1+a_{y_j}(g-1))\cdot R_{A_{j7}}\cdot R_{A_{j8}} \bmod n^2,$$

$$E_\varepsilon(a_{x_{j+1}})\equiv(1+a_{x_{j+1}}(g-1))\cdot R_{A_{j9}}\cdot R_{A_{j10}} \bmod n^2,\ E_\varepsilon(a_{x_j}a_{y_{j+1}})\equiv(1+a_{x_j}a_{y_{j+1}}(g-1))\cdot R_{A_{j11}}\cdot R_{A_{j12}} \bmod n^2.$$

(2) 将密文元组 $(E_\varepsilon(a_{y_{j+1}}),E_\varepsilon(a_{x_j}),E_\varepsilon(a_{y_j}a_{x_{j+1}}),E_\varepsilon(a_{y_j}),E_\varepsilon(a_{x_{j+1}}),E_\varepsilon(a_{x_j}a_{y_{j+1}}))$ 记作 $E_\varepsilon(A_j)$, 其中,$j\in\{1,2,\ldots,K-1\}$,对所有密文元组 $E_\varepsilon(A_1),E_\varepsilon(A_2),...,E_\varepsilon(A_{K-1})$ 做随机置换,并将所有的密文元组 $(E_\varepsilon(a_{y_{i+1}}),E_\varepsilon(a_{x_i}),E_\varepsilon(a_{y_i}a_{x_{i+1}}),E_\varepsilon(a_{y_i}),E_\varepsilon(a_{x_{i+1}}),E_\varepsilon(a_{x_i}a_{y_{i+1}}))\in\{E_\varepsilon(A_1),E_{\mathrm{E}}(A_2),...,E_\varepsilon(A_{K-1})\}$ 发给 Bob.

4. 对于 $i\in\{1,2,\ldots,K-1\}$,Bob 收到 $E_\varepsilon(a_{y_{i+1}}),E_\varepsilon(a_{x_i}),E_\varepsilon(a_{y_i}a_{x_{i+1}}),E_\varepsilon(a_{y_i}),E_\varepsilon(a_{x_{i+1}}),E_\varepsilon(a_{x_i}a_{y_{i+1}})$ 后,按照如下方式进行:

(1) 计算: $E_\varepsilon(b_xa_{y_{i+1}})\equiv(E_\varepsilon(a_{y_{i+1}}))^{b_x} \bmod n^2, E_\varepsilon(b_ya_{x_i})\equiv(E_\varepsilon(a_{x_i}))^{b_y} \bmod n^2.$

(2) 从云服务器上下载集合 R 后,随机选择 $k_b,r_{b_1}\in Z_n$, $2\ell(\ell\leqslant k)$个数: $R_1,R_2,...,R_\ell\in R,\chi_1,\chi_2,...,\chi_\ell,\chi_1',\chi_2',...,\chi_\ell'\in\{0,...,\ell\}$, 其中,$\ell$是一个比 1 大一些的小整数.并计算:

$$E_\varepsilon(r_{b1})=(1+r_{b1}\cdot k_b\cdot(g-1)\cdot R_1^{\chi_1}\cdot R_2^{\chi_2}\cdot\ldots\cdot R_\ell^{\chi_\ell} \bmod n^2,$$

$$E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b1})\equiv((E_\varepsilon(b_xa_{y_{i+1}})E_\varepsilon(b_ya_{x_i})E_\varepsilon(a_{y_i}a_{x_{i+1}}) \bmod n^2)^{k_b} \bmod n^2)E_\varepsilon(r_{b1}) \bmod n^2,$$

$$E_\varepsilon(b_xa_{y_i})\equiv(E_\varepsilon(a_{y_i}))^{b_x} \bmod n^2,$$

$$E_\varepsilon(b_ya_{x_{i+1}})\equiv(E_\varepsilon(a_{x_{i+1}}))^{b_y} \bmod n^2.$$

(3) 随机选择 $r_{b_2}\in Z_n$, 并计算:

$$E_\varepsilon(r_{b_2})=(1+r_{b_2}\cdot k_b\cdot(g-1)\cdot R_1^{\chi_1'}\cdot R_2^{\chi_2'}\cdot\ldots\cdot R_\ell^{\chi_\ell'} \bmod n^2,$$

$$E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b_2})\equiv((E_\varepsilon(b_xa_{y_i})E_\varepsilon(b_ya_{x_{i+1}})E_\varepsilon(a_{x_i}a_{y_{i+1}}))^{k_b} \bmod n^2)E_\varepsilon(r_{b_2}) \bmod n^2,$$

并将 $E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b_1}),E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b_2})$ 按随机顺序发给 Alice.

5. 对于 $i\in\{1,2,\ldots,K-1\}$,收到 $E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b_1}),E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b_2})$ 以后,Alice 计算:

$$\theta_i=\frac{\dfrac{L((E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b1}))^\lambda \bmod n^2)}{L(g^\lambda)}}{\dfrac{L((E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b2}))^\lambda) \bmod n^2}{L(g^\lambda)}}=\frac{L(E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b1}))^\lambda \bmod n^2)}{L((E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b2}))^\lambda \bmod n^2)}.$$

6. 通过判断θ_i与“1”的关系,确定 D_i 的符号:

$$Sign(D_i)=\begin{cases}1, & \theta_i>1\\ 0, & \theta_i=1\\ -1, & \theta_i<1\end{cases},$$

其中,$Sign(\cdot)$为符号函数.

7. 如果对于$\forall i\in\{1,2,\ldots,K-1\}$都有 $D_i\leqslant 0$,则返回“D=1”;否则,返回“D=0”.

3.3 保密社交意愿探测协议保密性分析

定理 3. 保密社交意愿探测协议可以安全地实现 Alice,Bob 两方的社交意愿探测.

证明:该协议安全与否的关键是协议执行后有没有造成参与者私有信息的泄露.接下来,我们将证明保密意愿探测协议在安全计算约谈意愿的过程中,Alice(持有凸多边形的活动区域 P,由顶点 $p_{a_1},p_{a_2},...,p_{a_K}$ 构成)、Bob (持有位置 p_b)两方除了得到“是否约谈”外,都无法获得有关对方私有数据的其他任何信息,即协议未给 Alice、Bob 两方造成信息泄露.

- 对于 Alice 数据的安全性

我们首先构造一个模拟保密探测协议执行的模拟器$\mathcal{S}_{\boldsymbol{B}}$.该模拟器的输入为:Alice 随机选择一个凸的活动区域 $p'_{a_1}, p'_{a_2}, ..., p'_{a_K}$, Bob 的私有位置 p_b,那么由模拟器$\mathcal{S}_{\boldsymbol{B}}$ 产生的视图为($p_b, E'_{\mathcal{E}}(a_{y_{i+1}}), E'_{\mathcal{E}}(a_{x_i}), E'_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E'_{\mathcal{E}}(a_{y_i}), E'_{\mathcal{E}}(a_{x_{i+1}}), E'_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$),其中,$1 \leqslant i \leqslant k$;而保密社交意愿探测协议的实际执行产生的视图为($p_b, E_{\mathcal{E}}(a_{y_{i+1}}), E_{\mathcal{E}}(a_{x_i}), E_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E_{\mathcal{E}}(a_{y_i}), E_{\mathcal{E}}(a_{x_{i+1}}), E_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$),其中 $1 \leqslant i \leqslant k$.因为 Alice 传输给 Bob 的信息是用自己的公钥$(n,n+1)$对自己的私有信息加密后的密文,又因方案$\mathcal{E}$已被证明在选择明文攻击下具有语义不可区分安全,所以由加密方案$\mathcal{E}$产生的密文是语义不可区分的,可得 $E'_{\mathcal{E}}(a_{y_{i+1}}), E'_{\mathcal{E}}(a_{x_i}), E'_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E'_{\mathcal{E}}(a_{y_i}), E'_{\mathcal{E}}(a_{x_{i+1}}), E'_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$ 与 $E_{\mathcal{E}}(a_{y_{i+1}}), E_{\mathcal{E}}(a_{x_i}), E_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E_{\mathcal{E}}(a_{y_i}), E_{\mathcal{E}}(a_{x_{i+1}}), E_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$ 是不可区分的.从而可得 $\mathcal{S}_{\boldsymbol{B}}(E'_{\mathcal{E}}(a_{y_{i+1}}), E'_{\mathcal{E}}(a_{x_i}), E'_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E'_{\mathcal{E}}(a_{y_i}), E'_{\mathcal{E}}(a_{x_{i+1}}), E'_{\mathcal{E}}(a_{x_i}a_{y_{i+1}}), p_b)$ 与真实视图 $view_{\boldsymbol{B}}^{\Pi}(E_{\mathcal{E}}(a_{y_{i+1}}), E_{\mathcal{E}}(a_{x_i}), E_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E_{\mathcal{E}}(a_{y_i}), E_{\mathcal{E}}(a_{x_{i+1}}), E_{\mathcal{E}}(a_{x_i}a_{y_{i+1}}), p_b)$ 是不可区分的,也就是说,满足定义关系式(2).

- 对于 Bob 位置信息的私密性

我们构造一个 Bob,输入其私有位置信息以及由其随机选择的 $k_b, r_{b_1}, r_{b_2} \in Z_n$, 就能模拟 Alice 视图的模拟器$\mathcal{S}_{\boldsymbol{A}}$.于是,由模拟器$\mathcal{S}_{\boldsymbol{A}}$产生的视图为

$$(p_{a_1}, p_{a_2}, ..., p_{a_K}, E_{\mathcal{E}}(k_b(b_x a_{y_{i+1}} + b_y a_{x_i} + a_{y_i}a_{x_{i+1}}) + r_{b_1}), E_{\mathcal{E}}(k_b(b_x a_{y_i} + b_y a_{x_{i+1}} + a_{x_i}a_{y_{i+1}}) + r_{b_2}), D).$$

因密文 $E_{\mathcal{E}}(k_b(b_x a_{y_{i+1}} + b_y a_{x_i} + a_{y_i}a_{x_{i+1}}) + r_{b_1}), E_{\mathcal{E}}(k_b(b_x a_{y_i} + b_y a_{x_{i+1}} + a_{x_i}a_{y_{i+1}}) + r_{b_2})$ 是 Bob 由密文 $E_{\mathcal{E}}(a_{y_{i+1}}), E_{\mathcal{E}}(a_{x_i}), E_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E_{\mathcal{E}}(a_{y_i}), E_{\mathcal{E}}(a_{x_{i+1}}), E_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$ 通过同态运算计算得到的,Alice 获得 $E_{\mathcal{E}}(k_b(b_x a_{y_{i+1}} + b_y a_{x_i} + a_{y_i}a_{x_{i+1}}) + r_{b_1}), E_{\mathcal{E}}(k_b(b_x a_{y_i} + b_y a_{x_{i+1}} + a_{x_i}a_{y_{i+1}}) + r_{b_2})$ 后,通过解密运算,最多只能得到两个各包含 5 个未知数的方程,通过联立方程组计算出具体的 (b_x, b_y) 是不可行的,故 $(p_{a_1}, p_{a_2}, ..., p_{a_K}, E_{\mathcal{E}}(k_b(b_x a_{y_{i+1}} + b_y a_{x_i} + a_{y_i}a_{x_{i+1}}) + r_{b_1}), E_{\mathcal{E}}(k_b(b_x a_{y_i} + b_y a_{x_{i+1}} + a_{x_i}a_{y_{i+1}}) + r_{b_2}), D)$ 与实际执行中的视图是计算不可区分的,即满足安全定义中的等式(1).

综上所述,Alice 和 Bob 的私密性满足安全定义的形式化等式(1)和等式(2).所以,保密社交意愿探测协议可以安全地实现 Alice、Bob 两方社交意愿的探测. □

4 保密社交意愿探测协议效率分析

不失一般性,我们假定 Alice 和 Bob 为文献[1]的协议和本文协议的参与者,并假定 Bob 的坐标为(b_x,b_y),Alice 提供的意愿区域为 K 个顶点构成的凸多边形.为了进行公平比较,此处将执行协议时花费的总开销统一用一次自模乘运算($r_x^2 \mod n^2$)作为统计的基本单位.

Alice 和 Bob 在执行文献[1]的协议时,总共至少需要 $K(8n+b_x+b_y+2\lambda)$次自模乘运算($r_x^2 \mod n^2$).因为基于云外包计算的同态加密方案$\mathcal{E}$中的计算 $R_i = r_i^n \mod n^2$ 可以在预处理阶段由云服务器完成,并且 Alice 和 Bob 在预处理阶段可以随时随地地从云服务器下载集合 $R = \{R_i \mid R_i = r_i^n \mod n^2\}$,所以得到集合 $R = \{R_i \mid R_i = r_i^n \mod n^2\}$ 的时间可以忽略不计;又因为 Alice 和 Bob 在得到集合 $R = \{R_i \mid R_i = r_i^n \mod n^2\}$ 后,利用集合中的元素,通过执行有限次的模乘运算($r_x^2 \bmod n^2$),即可秘密地得到 $r_x^n \mod n^2$, 不再需要做 n 次自模乘运算($r_x^2 \mod n^2$).因此,基于同态加密方案$\mathcal{E}$的保密社交意愿探测协议时,Alice 和 Bob 总计需要花费 $K(18+2b_x+2b_y+2k_b+2(\ell+2)+2\lambda)$次自模乘运算($r_x^2 \mod n^2$).显然,本文的协议比文献[1]的协议在运算效率上有了质变性的提升.

基于同态加密方案$\mathcal{E}$的保密社交意愿探测协议可以解决 Alice 出具的 K 个顶点相邻顶点坐标差小于 0 的情形;而对于文献[1]的协议而言,当 Alice 出具的 K 个顶点相邻顶点坐标差小于 0 时,它无法正确运行.此外,文献[1]的协议只能用于解决实时位置的近感探测问题,已经不能满足社交网络用户新的个性化需求;而本协议不仅可以用于彻底解决文献[1]的协议提出的近感探测问题,还能满足社交网络用户日益增长的个性化需求:保密社交筹划,即保密社交意愿探测,解决的是保密探测领域中的新问题.下表是保密社交探测协议和协议在效率(用执行协议时各参与方在加密和解密算法中花费的计算开销总和体现)、解决问题的能力(从能否解决保密探测区域相邻两点坐标差商小于 0 的情形体现)以及能够解决的问题这 3 个方面的对比.保密探测协议与文献[1]的协

议的对比分析见表 2.

Table 2 Comparative analysis on private social-willing test and the protocol of Ref.[1]

表 2 保密探测协议与文献[1]的协议的对比分析

类型	Alice 和 Bob 总开销 (自模乘运算($r_x^2 \bmod n^2$)次数)	解决问题的能力(能否解决保密探测区域相邻两点坐标差商小于 0 的情形)	能解决的问题
文献[1]的协议	至少为 $K(8n+b_x+b_y+2\lambda)$	×	保密近感探测
本协议	$K(18+2b_x+2b_y+2k_b+2(\ell+2)+2\lambda)$	√	保密社交意愿探测 保密近感探测

√表示具有某种性能,×表示不具有某种性能

5 结束语

本文对保密意愿探测问题进行了研究.为了高效地解决这一问题,首先设计了一个带云辅助计算的同态加密方案;然后,利用该加密方案设计了一个高效的保密意愿探测协议.分析结果表明,此协议在效率和安全性方面都优于先前的类似协议,并且其安全性是在标准的 ideal/real 模型下实现的.

References:

[1] Mu B, Bakiras S. Private proximity detection for convex polygons. Tsinghua Science and Technology, 2016,21(3):270−280.

[2] Jing T, Lin P, Lu Y, Hu C, Huo Y. FPODG: A flexible and private proximity testing based on'one degree' grid. Int'l Journal of Sensor Networks, 2016,20(3):199−207.

[3] Zheng Y, Li M, Lou WJ, Hou T. Location based handshake and private proximity test with location tags. IEEE Trans. on Dependable and Secure Computing, 2017,14(4):406−419.

[4] Faber S, Petrlic R, Tsudik G. Unlinked: Private proximity-based off-line OSN interaction. In: Proc. of the 14th ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2015. 121−131.

[5] Kotzanikolaou P, Patsakis C, Magkos E, Michalis K. Lightweight private proximity testing for geospatial social networks. Computer Communications, 2016,73:263−270.

[6] Zhuo G, Jia Q, Guo L, Li M, Fang Y. Privacy-preserving verifiable proximity test for location-based services. In: Proc. of the 2015 IEEE Global Communications Conf. (GLOBECOM). New York: IEEE Press, 2015. 1−6.

[7] Gong X, Chen X, Xing K, Shin D, Zhang M, Zhang J. Personalized location privacy in mobile networks: A social group utility approach. In: Proc. of the 2015 IEEE Conf. on Computer Communications (INFOCOM). New York: IEEE Press, 2015. 1008−1016.

[8] Werner M. Privacy-protected communication for location-based services. Security and Communication Networks, 2016,9(2): 130−138.

[9] Zhong G, Goldberg I, Hengartner U. Louis, Lester and Pierre: Three protocols for location privacy. In: Proc. of the Int'l Workshop on Privacy Enhancing Technologies. Berlin, Heidelberg: Springer-Verlag, 2007. 62−76.

[10] Narayanan A, Thiagarajan N, Lakhani M, Michael H, Boneh D. Location privacy via private proximity testing. In: Proc. of the 18th Annual Network & Distributed System Security Symp. (NDSS 2011). IETF, 2011. 1−17.

[11] Šikšnys L, Thomsen JR, Šaltenis S, Yiu M, Andersen O. A location privacy aware friend locator. In: Proc. of the Int'l Symp. on Spatial and Temporal Databases. Berlin, Heidelberg: Springer-Verlag, 2009. 405−410.

[12] Šikšnys L, Thomsen JR, Šaltenis S, Yiu M. Private and flexible proximity detection in mobile social networks. In: Proc. of the 2010 11th IEEE Int'l Conf. on Mobile Data Management (MDM). New York: IEEE Press, 2010. 75−84.

[13] Mascetti S, Freni D, Bettini C, Wang X, Jajodia S. Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies. The VLDB Journal—The Int'l Journal on Very Large Data Bases, 2011,20(4):541−566.

[14] Hallgren P, Ochoa M, Sabelfeld A. Innercircle: A parallelizable decentralized privacy-preserving location proximity protocol. In: Proc. of the 2015 13th IEEE Annual Conf. on Privacy, Security and Trust (PST). New York: IEEE Press, 2015. 1−6.

[15] Patsakis C, Kotzanikolaou P, Bouroche M. Private proximity testing on steroids: An NTRU-based protocol. In: Proc. of the Int'l Workshop on Security and Trust Management. Berlin, Heidelberg: Springer-Verlag, 2015. 172−184.

[16] Halevi T, Ma D, Saxena N, Xiang T. Secure proximity detection for NFC devices based on ambient sensor data. In: Proc. of the European Symp. on Research in Computer Security. Berlin, Heidelberg: Springer-Verlag, 2012. 379–396.

[17] Zhuo G, Jia Q, Guo L, Li M, Fang Y. Privacy-preserving verifiable proximity test for location-based services. In: Proc. of the 2015 IEEE Global Communications Conf. (GLOBECOM). New York: IEEE Press, 2015. 1–6.

[18] Nielsen JD, Pagter JI, Stausholm MB. Location privacy via actively secure private proximity testing. In: Proc. of the 2012 IEEE Int'l Conf. on Pervasive Computing and Communications Workshops (PERCOM Workshops). New York: IEEE Press, 2012. 381–386.

[19] Niu B, Zhang T, Zhu X, Li H, Lu Z. Priority-aware private matching schemes for proximity-based mobile social networks. arXiv preprint arXiv:1401.8064, 2014. https://arxiv.org/pdf/1401.8064

[20] Shrestha B, Saxena N, Truong HTT, Asokan N. Contextual proximity detection in the face of context-manipulating adversaries. arXiv preprint arXiv:1511.00905, 2015. https://arxiv.org/pdf/1511.00905.pdf

[21] Li HP, Hu H, Xu J. Nearby friend alert: Location anonymity in mobile geosocial networks. IEEE Pervasive Computing, 2013,12(4): 62–70.

[22] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 1999. 223–238.

[23] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985,31(4):469–472.

[24] Thomas T. Secure two-party protocols for point inclusion problem. arXiv preprint arXiv:0705.4185, 2007. https://arxiv.org/pdf/0705.4185.pdf

[25] Yang B, Shao ZY, Zhang WZ. Secure two-party protocols on planar convex hulls. Journal of Information, 2012,9(4):915–929.

[26] Yun Y, Liusheng H, Wei Y, Youwen Y. Efficient protocols for point-convex hull inclusion decision problems. Journal of Networks, 2010,5(5):559–567.

[27] 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 with English abstract). http://www.jos.org.cn/1000-9825/5239.htm [doi: 10.13328/j.cnki.jos.005239]

[28] Katz J, Lindell Y. Introduction to Modern Cryptography. 2nd ed., New York: CRC Press, 2014. 389–398.

[29] Atallah MJ, Du W. Secure multi-party computational geometry. In: Proc. of the Workshop on Algorithms and Data Structures. Berlin, Heidelberg: Springer-Verlag, 2001. 165–179.

附中文参考文献:

[27] 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 [doi: 10.13328/j.cnki.jos.005239]

巩林明(1975－),男,山东青岛人,博士,讲师,主要研究领域为公钥密码,安全多方计算.

窦家维(1963－),女,博士,副教授,主要研究领域为公钥密码,应用数学.

李顺东(1963－),男,博士,教授,博士生导师,主要研究领域为公钥密码,安全多方计算.

王道顺(1964－),男,博士,副教授,博士生导师,主要研究领域为密码算法,视频智能行为分析,多媒体安全与取证.