隐私保护的点与多边形位置关系判定协议

朱如锦 杨 波
(华南农业大学信息学院 广州 510642)

摘 要 隐私保护的计算几何是安全多方计算的一个全新研究领域。针对已有的安全判定点与多边形位置关系协议的缺陷,在半诚实模型下,提出基于铅垂线算法和不经意传输协议的隐私保护的点与多边形位置关系判定协议,并对该协议的正确性、计算复杂性、通信复杂性和安全性进行了分析和证明。新的协议不仅可以在实数域中使用,不局限于凸多边形,而且能适用于多边形带孔的情况。

关键词 安全多方计算,计算几何,多边形,铅垂线算法,不经意传输协议
中图法分类号 TP398 **文献标识码** J

Relative Position Determination of Point and Polygon with Privacy Preserving

ZHU Ru-jin YANG Bo
(College of Informatics, South China Agricultural University, Guangzhou 510642, China)

Abstract Privacy preserving computational geometry is a new research branch of secure multiparty computation. Because of the shortcomings and restraints in existing protocols, in semi-honest, a new protocol based on plumb line algorithm and oblivious transfer protocol for relative position determination of point and polygon was proposed in this paper. The correctness, computation efficient and security were analyzed and proved in this paper as well. The new protocol not only can be used in real number field, but also can be used in any polygon with great efficient.

Keywords Secure multiparty computation, Computational geometry, Polygon, Plumb line algorithm, Oblivious transfer

1 引言

安全多方计算(Secure Multiparty Computation, SMC)[1],是研究一组互不信任的参与者之间保护隐私信息的合作计算问题。近年来,该问题已成为国内外信息安全学者研究的热点之一。1982年由A. C Yao[2]首次提出来后,已经得到了一些不错的理论成果[3-7],其应用领域涵盖了科学计算与统计分析、计算几何、数据挖掘、信息检索等。由于受到计算复杂度和通信复杂度的双重制约,想构造一般通用的方法来解决现实中的实际问题是不现实的。对于特殊的应用协议,需要对通用的方法进行有效剪裁来提高协议的适应性、实用性和高效性[1]。

保护隐私的计算几何(Privacy Preserving Computational Geometry, PPCG)是安全多方计算的一个重要分支,其主要研究的是分布式网络中计算几何的信息安全和隐私保护的问题。文献[7]中,作者Du和Atallah首次引入了保护隐私计算几何的概念,并指出它在军事、商业等领域有着广泛的应用前景。他们提出安全两方点乘协议,并在此基础上研究和解决了点与线关系、点与多边形关系、线段与线段关系、线段与多边形以及多边形与多边形保护隐私位置关系判定的问题[7]。安全两方点乘协议在PPCG中有着重要的应用,此后很多的协议方案都是基于这个协议实现的[8-11]。

本文分析和比较了不同的点与多边形位置关系判定算法,将铅垂线算法应用到保护隐私的点与多边形位置关系判定问题中,并结合了不经意传输协议进行两方安全判定协议的设计。与此前的协议相比较,不仅在效率上得到了提升,而且应用范围也拓展到了实数域,并能适应于任意多边形的情况(包括凸、凹、带孔的多边形)。

本文假设参与计算的双方都是半诚实的,即参与的双方严格遵照协议的规程来进行,不会出现中途强行退出或者恶意掺入虚假信息的行为。但是执行的双方可能是好奇的,他们会保存和收集协议执行过程中的信息,并期望能从这些信息中推算对方的隐私信息。

2 预备知识

这里将介绍该协议中需要使用的一个算法、一个SMC基础协议以及半诚实模型下协议安全性的定义。

算法1 铅垂线段与给定线段相交计算

已知铅垂线 l_1 顶点分别为 $A_1(x,y_a)$、$A_2(x,y_b)$(横坐标相同,$y_a>y_b$,即 A_1 点在 A_2 点上方),给定线段 l_2 顶点分别为 $B_1(x_1,y_1)$和 $B_2(x_2,y_2)$(满足 $y_1>y_b$ 且 $y_2>y_b$),判断 l_1 和 l_2 是否相交,具体算法步骤如下:

(1) 如果 x 不属于区间$[x_1,x_2]$,则断定 l_1 与 l_2 不相交,结束;否则继续(2);

本文受国家自然科学基金(60773175和60973134),现代通信国家重点实验室基金(9140C1108020906),广东省自然科学基金(1035180600100 0000,10151064201000028和9151064201000058)资助。

朱如锦(1985—),男,硕士生,主要研究方向为安全多方计算,E-mail:zhu_rujin@hotmail.com。

(2) 如果 $y_a<y_1$ 且 $y_a<y_2$，则断定 l_1 与 l_2 不相交，结束；否则继续(3)；

(3) 通过两点 B_1 和 B_2 易得过这两点的直线方程 $ax+by+c=0$，如果将 $A_1(x,y_a)$ 点坐标带入直线方程：①满足 $ax+by+c\geqslant 0$，则 l_1 与 l_2 相交；②满足 $ax+by+c<0$，则 l_1 与 l_2 不相交；结束。

协议 1　$1-out-of-m$ 不经意传输协议(Oblivious Transfer，OT_m^1)[10]

Alice 将 n 个消息 $m_1,m_2,\cdots,m_n$ 发送给 Bob，协议执行后 Bob 只得到其中的一个消息(对 Alice 的隐私性)，Alice 并不知道 Bob 选择的是哪一个消息(对 Bob 隐私性)，Bob 可以确信他得到了想要的消息(正确性)。本文将使用文献[12]中的高效的 $1-out-of-m$ 不经意传输协议，具体协议情况如下：

系统参数：(g,h,G_q)，G_q 是一个 q 阶循环群，g、h 是 G_q 的两个生成元，而且 $\log_g^h$ 保密。

初始化：发送者 Alice 的输入为：$m_1,m_2,\cdots,m_n\in G_q$；接受者 Bob 的选择为 α，$1\leqslant\alpha\leqslant n$。

交互步骤：

Bob 发送 $y=g^r h^\alpha$，$r\in_R Z_q$。Bob 向 Alice 承诺要选择的消息 m_α。

Alice 发送 $c_i=(g^{k_i},m_i(y/h^i)^{k_i})$，$k_i\in_R Z_q$，$1\leqslant i\leqslant n$。Alice 将消息序列进行有效的隐藏。

Bob 获得 $c_\alpha=(a,b)$，计算 $m_\alpha=b/a^r$。Bob 只能计算得到他承诺的消息，其他都是无意义的信息。

协议的算法复杂度分析：Bob 只需要 2 个模指数运算——计算 y 和 a^r；Alice 需要 3 个模指数运算——计算 a，y^k 和 h^k，而且 a 和 h^k 都是可以被预先计算的，所以该协议是高效的。

安全定义：在半诚实模型下，假设参与计算的双方分别为 Alice 和 Bob，设 $f=(f_1,f_2)$ 是一个概率多项式时间的函数，Π 则是参与合作计算的协议。运行协议 Π 的过程中，参与者 Alice 和 Bob 所到的消息序列分别记为视图 $View_1^\Pi(x,y)=(x,r,m_1^1,m_2^1,\cdots,m_t^1)$、$View_2^\Pi(x,y)=(y,r,m_1^2,m_2^2,\cdots,m_t^2)$，其中 r 为双方共同产生的随机数，双方接收到的第 i 个消息分别记为 m_i^1、m_i^2。执行协议后，双放的输出为 $Output_1^\Pi(x,y)$ 和 $Output_2^\Pi(x,y)$，显然 $Output$ 的输出结果包含于 $View$ 的通信消息序列之中。

对于一个函数 f，如果存在概率多项式时间算法 S_1，S_2 使得：

$$\{S_1(x,f_1(x,y),f_2(x,y))\}\equiv\{View_1(x,y),Output_2(x,y)\}$$

$$\{f_1(x,y),S_2(x,f_2(x,y))\}\equiv\{Output_1(x,y),View_2(x,y)\}$$

则可以认为协议 Π 保密地计算 f，参与的双方能够得到的信息仅可以通过他自己的输入和输出信息模拟出来，不能获得额外的信息，其中“≡”表示不可区分，所以要证明一个协议方案是保密的需要构造出模拟器 S_1 和 S_2[13]。

3　基于隐私保护的点与多边形关系判定协议

3.1　问题定义

隐私保护的点与多边形位置关系判定问题可以描述为，参与协议的双方分别为 Alice 和 Bob，Alice 拥有自己的隐私点 $P(x_p,y_p)$，Bob 拥有一个私有多边形 G(G 可以为任意多边形)，多边形内部可以拥有孔 H(假设孔可以是规则的圆形、椭圆形或者是任意的多边形)，多边形的 n 个顶点分别定义为 $P_1(x_1,y_1)$，$P_2(x_2,y_2)$，$\cdots$，$P_n(x_n,y_n)$。

3.2　铅垂线判断点与多边形算法

从图 1 中可以得到一个简单的定理：(1)如果点在多边形内部，过点的铅垂线与多边形的边的交点个数是奇数；(2)如果点在多边形外，则过点的铅垂线与多边形的交点个数就是偶数。

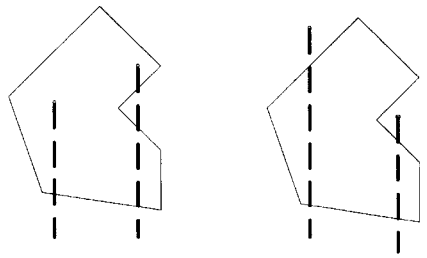

图 1　铅垂线判断点与多边形位置关系

铅垂线与多边形相交的特殊的情况包括：①铅垂线与多边形的顶点相交；②铅垂线与多边形的边部分重合。针对情况①的解决方法，需要同时判断该顶点相邻两条边是否都在铅垂线的同一侧。如果是，则交点个数加 2；否则交点数加 1。针对情况②的解决方法，首先需要判断点是否在直线上，如果是，则点在多边形内；否则继续与情况①的判定情况类似。与铅垂线重合的边相邻的两条边，如果同侧，则交点个数加 2，否则加 1。如图 2 所示，上述方法可以容易推广到带孔的任意多边形情况，同样适用于以上的定理。

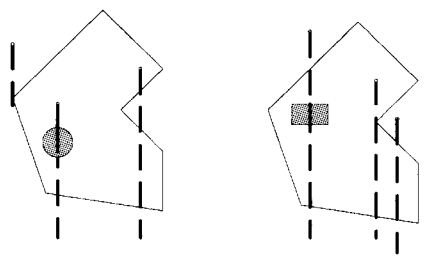

图 2　铅垂线判断点与带孔多边形位置关系

3.3　判定协议

在协议执行之前，Bob 预先在多边形 G 顶点集合 $P_i(x_i,y_i)$ 中找到最小和最大的纵坐标和横坐标，分别记作 $y_{\min}$、$y_{\max}$ 和 $x_{\min}$、$x_{\max}$，并在区间 $y<y_{\min}$ 中随机选取一个值 y_r 作为铅垂线段的下垂边界。因此，通过上面的计算，容易得到多边形的最小外接矩形，其中横左边和纵坐标的范围分别是$[x_{\min},y_{\max}]$和$[y_{\min},y_{\max}]$，算法复杂度为 $O(n)$(n 为多边形的顶点个数)。由此，本文提出基于铅垂线算法和 OT_m^1 协议的点与任意多边形的位置关系判定协议。

输入：Alice 输入为其私有信息点 $P(x_p,y_p)$，Bob 输入为 y_r 和多边形 G 的顶点序列 $P_1(x_1,y_1)$，$P_2(x_2,y_2)$，$\cdots$，$P_n(x_n,y_n)$，m 为双方协商的系统安全参数。

输出：Alice 的私有信息点 $P(x_p,y_p)$ 是否在 Bob 拥有的多边形 G 内。

(1) Alice 选取出 m 个随机点 $P_i^r(x_i^r,y_i^r)$，$1\leqslant i\leqslant m$，发送

给 Bob，其中 $i=x$ 为 Alice 拥有的隐私点 P。

(2) Bob 将接收到的 m 个点与 y_r 构造的 m 条铅垂线段记为 $P_i^rQ_i^r$，其中线段两个顶点分别是 $P_i^r(x_i^r, y_i^r)$ 和 $Q_i^r(x_i^r, y_r)$，两点的横坐标是相同的 x_i^r。然后调用算法 1 分别计算判定 m 线段与多边形 G 的各条边是否相交，包括多边形内部的孔，并记录下其相交的次数 c_i。然后将所有相交结果通过 OT_m^1 不经意传输协议发送回给 Alice。

(3) 通过 OT_m^1 不经意传输协议后，保证 Alice 能且只能获得 c_x 的值，Bob 对于 Alice 所得到的值一无所知。Alice 对获得的值进行计算，若 c_x 为偶数，则点 P 在多边形外，否则点 P 在多边形内。最后，Alice 将结果告诉 Bob。

3.4 协议分析

定理 1 基于铅垂线算法的点与任意多边形的位置关系判定协议是安全的。

证明：(正确性)基于算法 1 的正确性，Bob 通过 Alice 发送过来的 m 个点序列，构造出 m 条铅垂线段，并使用算法 1 判定铅垂线与多边形 G 各条边是否有交点，并记录下交点的个数。然后，通过 OT_m^1 不经意传输协议将交点个数 c_i 发送回给 Alice。基于 OT_m^1 协议 Alice 确定接收到自己需要的 c_x，最后根据 c_x 的奇偶性，来判断自己的私有信息点 P 是否在多边形内，再与 Bob 共享协议执行的结果。

(安全性) 由安全性的定义得，需要证明协议是安全的首先要构造模拟器 S_1 和 S_2。

证明：首先构造铅垂线和多边形的边相交时的 S_1 和 S_2，其中谓词可以定义为：

$$F(l_1, l_2)=\begin{cases}1 & \text{当 1 的时候，} l_1 \text{ 和 } l_2 \text{ 相交，不相交则为 0}\\ 0\end{cases}$$

式中，l_1 为铅垂线段，l_2 为多边形 G 的边。所以，产生的消息序列表示为：

$$\begin{aligned}&View_1^{\Pi}(l_1, l_2)\\&=(l_1, r, (l_1^0, \cdots, l_n^0), (M_1, \cdots, M_m), F(l_1, l_2), f_1(l_1, l_2))=f_2(l_1, l_2)=Output_1^{\Pi}(l_1, l_2)=Output_2^{\Pi}(l_1, l_2)\\&=F(l_1, l_2)\end{aligned}$$

式中，l_1 是是输入，r 是 Alice 的随机掷币结果，M_i 是 OT_m^1 不经意传输协议需要计算的 $f(l_1, l_2)$ 的数据信息。首先，构造 S_1 来模拟 $View_1^{\Pi}(l_1, l_2)$ 使得安全定义中的式(1)成立。

模拟过程如下：

(1) S_1 接收 $(l_1, f_1(l_1, l_2))$ 作为 Alice 的输入，根据 $f_1(l_1, l_2)$ 的值，确定线段 l_2'，使 $f_1(l_1, l_2)=f_1(l_1, l_2')$。$S_1$ 计算数组 $Y'=\{y_1', \cdots, y_m'\}$，其中 $y_1'=f_1(l_{1i}, l_2')$。

(2) 模拟 OT_m^1 不经意传输过程，S_1 可以得到一组 M_1'，$\cdots$，M_m'，并根据这一组的 M_1'，$\cdots$，M_m' 计算得到 $f_1(l_1, l_2')$，根据构造的过程知道 $f_1(l_1, l_2)=f_1(l_1, l_2')$。$OT_m^1$ 不经意传输过程的安全已经得到了证明[12]。

首先，Alice 将个人信息进行了有效的隐藏，将随机产生的 m 个信息点发送给 Bob，其中只有一个点是 Alice 真正的私有信息点。所以，Bob 能正确地猜测到 Alice 的个人私有信息的概率仅为 $1/m$，从而有效地保证了 Alice 私有信息不被 Bob 得知。Bob 通过 OT_m^1 不经意协议将结果发送给 Alice 的时候，Alice 仅得到自己私有信息过 P 点的铅垂线与多边形的交点的个数，除此之外，Alice 得不到其他任何信息。因此，该协议有效地保护了 Bob 私有多边形 G 的信息。

综上所述，Alice 和 Bob 在保护隐私的点与多边形关系判定协议中，不能获得对方的具体输入信息，并且能够正确地判定点与任意多边形的位置关系，因此协议是安全的。

(复杂性) 计算复杂度 在协议预处理阶段，Bob 需要找其拥有多边形 G 的最小外接矩形，并随机选取 y_r，需要的时间复杂度为 $O(n)$。在协议第二步需要计算和统计 Alice 发送过来的 m 个信息点产生的铅垂线与多边形 G 的交点个数，其间需要调用算法 1 的次数为 $m*n$，若多边形内部有孔的边数 n'，则第二步需要计算的次数为 $m*(n+n')$，算法复杂度为 $O(\max(m,n)^2)$。Alice 随机发送 m 个坐标点的时间复杂度为 $O(m)$，协议最后判断接收的 c_x 的奇偶性为 $O(1)$，算法复杂度为 $O(m)$。协议双方 Alice 和 Bob 需要调用子协议 OT_m^1 不经意传输协议一次。

(通信复杂度) OT_m^1 不经意传输协议一次，Alice 发送 m 个坐标点对。

综上所述，该协议避免了使用计算复杂度高的点积协议和百万富翁比较协议，使得协议的性能得到了一定程度的提升。而且，在调用 OT_m^1 不经意传输协议的时候只返回了铅垂线与多边形 G 的交点的个数，可以使用基于 DDH(Decision Diffie-Hellman) 困难假设的 OT_m^1 不经意传输协议，例如文献[14]。在判断铅垂线与多边形的边相交的情况，算法 1 不局限在整数域上，对任意多边形都能很好地适应，对比文献[4,15]有较大的优势和更强的灵活性、适应性以及应用范围。

3.5 协议算法的改进

在协议预处理阶段，Bob 可以快速计算得到其拥有的多边形 G 的最小外接矩形 R_0 和最小内接矩形 R_i。在执行协议阶段，获得 Alice 发送过来的 m 个坐标点对时，可以快速计算判断得到这些点的大概位置，从而避免了多次使用算法 1 对所有多边形 G 的各条边进行计算和判定，能有效地降低算法的复杂度。例如具体实现过程可以参考：如果 Alice 发过来的点 $P_i^r(x_i^r, y_i^r)$ 在 R_0 外，$c_i=0$；如果点 $P_i^r(x_i^r, y_i^r)$ 在 R_i 内，$c_i=1$；如果 $P_i^r(x_i^r, y_i^r)$ 在 R_0 内 R_i 外，才需要调用算法 1。

结束语 本文将铅垂线算法和不经意传输协议相结合，提出了新的保护隐私的点和多边形位置关系判定协议。摒弃了以往使用复杂度高和安全性差的两方安全点乘协议，使得本文中的协议可以应用到更广的范围，与之前的协议相比较数据不再局限在整数范围内、不要求多边形是凸多边形以及可以适用于带孔的多边形，从而提高了其适应性和灵活性。

参 考 文 献

[1] Goldreich O. Foundations of Cryptography: Volume II, Basic Applications [M]. Cambridge: Cambridge University Press, 2004

[2] Yao A C. Protocols for secure computations [A]// Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science [C]. Chicago, USA, 1982: 160-164

[3] Du Wen-liang, Atallah M J. Privacy-preserving cooperative scientific computations[C]// 14th IEEE Computer Security Foundations Workshop. Nova Scotia, Canada, June 2001: 11-13

[4] Luo W J, Li X. A study of secure multi-party statistical analysis [C]// Proceeding of IEEE International Conference on Computer Networks and Mobile Computing. Shanghai, 2003: 377-382

(下转第 43 页)

$ID_{B_n}^*\}, w^*, p\sigma^*)$，如果满足下面3个条件，则该签名是有效的。

• $\mathcal{MPV}(m^*, (ID_A^*, \{ID_{B_1}^*, ID_{B_2}^*, \cdots, ID_{B_n}^*\}, w^*, p\sigma^*)) = \text{Accept}$；

• (ID_A^*)没有提交用户私钥询问；

• $ID_A^* \neq ID_{B_i}^*$ $(i \in \{1,2,\cdots,n\})$，并且$(ID_A^*, w^*) \notin delList$。

如果$\mathcal{A}$伪造的签名是有效的，则游戏返回1，否则返回0。

我们将上述游戏的运行结果记为$Gm_{IBMPS,\mathcal{A}}^{UF\text{-}CMIA}(k)$，则敌手$\mathcal{A}$在上述游戏中的优势可定义为

$$Adv_{IBMPS,\mathcal{A}}^{UF\text{-}CMIA}(k) = \Pr[Gm_{IBMPS,\mathcal{A}}^{UF\text{-}CMIA}(k) = 1]$$

其中概率是在敌手和挑战者随机抛币下得到的。

对于一个IBMPS方案来说，如果敌手$\mathcal{A}$在上述游戏中的优势至少为ε、运行时间至多为t，并且敌手$\mathcal{A}$提交用户私钥询问的次数至多为q_e、授权询问的次数至多为q_d、签名询问的次数至多为q_s，则敌手$\mathcal{A}$被称为该IBMPS方案的$(\varepsilon, t, q_e, q_d, q_s)$-伪造者；如果这样的$(\varepsilon, t, q_e, q_d, q_s)$-伪造者不存在，则该IBMPS方案被称为$(\varepsilon, t, q_e, q_d, q_s)$-安全的。

可以看出，在上面的模型中，伪造情形②是敌手在不知道一个代理签名人的私钥而知道原始签名人的私钥和其余的代理签名人的私钥时对多重代理签名的伪造；伪造情形③是敌手在不知道原始签名人的私钥而知道所有代理签名人的私钥时对多重代理签名的伪造。因此我们提出的模型完全符合代理签名对强不可伪造性[10,11]的要求。另外，代理签名的安全定义[5]通过一种通用构造方法说明它是可达到的。我们的安全定义也可用类似的方法说明它是可达到的。

结束语 代理签名一提出就受到国内外学者的广泛关注，多重代理签名是代理签名的重要的扩展形式。将多重代理签名与基于身份的密码学结合起来，人们提出了一些基于身份的多重代理签名方案。可是，因为没有基于身份的多重代理签名的安全模型，所以这些方案都没有提供正式的安全性证明。本文形式化地定义了基于身份的多重代理签名，然后提出了一个基于身份的多重代理签名的安全模型。这为以后设计可证安全的基于身份的多重代理签名方案提供了重要的保证。

参考文献

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation[C]// Proceedings of the 3rd ACM Conference on Computer and Communications Security (CCS'96). New York: ACM Press, 1996: 48-57

[2] Hwang S, Shi C. A simple multi-proxy signature scheme[C]// Proceedings of the 10th National Conference on Information Security. Hualien, Taiwan, 2000: 134-138

[3] Boldyreva A, Palacio A, Warinschi B. Secure proxy signature schemes for delegation of signing rights[R]. Cryptology ePrint Archive. Report 2003/096, 2003. http://eprint.iacr.org/

[4] Malklin T, Obana S, Yung M. The hierarchy of key evolving signatures and a characterization of proxy signatures[C]// Proceedings of Eurocrypt 2004, Lecture Notes in Computer Science 3027. Berlin: Springer-Verlag, 2004: 306-322

[5] Schuldt J C N, Matsuura K, Paterson K G. Proxy signatures secure against proxy key exposure[C]// Proceedings of Public Key Cryptography 2008 (PKC'08), Lecture Notes in Computer Science 4939. Berlin: Springer-Verlag, 2008: 141-161

[6] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of Crypto 1984, Lecture Notes in Computer Science 196. Berlin: Springer-Verlag, 1984: 47-53

[7] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// Proceedings of Crypto 2001, Lecture Notes in Computer Science 2139. Berlin: Springer-Verlag, 2001: 213-229

[8] Chen X, Zhang F, Kim K. ID-based multi-proxy signature and blind multisignature from bilinear pairings[C]// Proceedings of KIISC (Korea Institute of Information Security and Cryptology) Conference 2003. Korea, 2003, 11-19

[9] Li X, Chen K. ID-based multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes from bilinear pairings[J]. Applied Mathematics And Computation, 2005, 169 (1): 437-450

[10] Lee B, Kim H, Kim K. Strong proxy signature and its applications[C]// Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS'01). Oiso, Japan, 2001: 603-608

[11] Lee B, Kim H, Kim K. Secure mobile agent using strong non-designated proxy signature[C]// Proceedings of the 6th Australasian Conference on Information Security and Privacy (ACISP'01). Lecture Notes in Computer Science 2119. Berlin: Springer-Verlag, 2001: 474-486

(上接第40页)

[5] Lin H Y, Tzengw G. An efficient solution to the millionaires' problem based on homomorphic encryption [M]. Applied Cryptography and Network Security, LNCS 3531. Berlin: Springer-Verlag, 2005: 456-466

[6] Brankovic L, Estivill-Castro V. Privacy Issues in Knowledge Discovery and Data Mining [C]// Melbourne, Victoria, Australia: Proc. of Australian Institute of Computer Ethics Conference. 1999

[7] Atallah M J, Du W L. Secure multi-party computational geometry [C]// Dehne F K H A, Sack J R, T amassial R. Proceedings of Seventh International Workshop on Algorithms and Data Structures. London: Springer-Verlag, 2001: 165-179

[8] Li Shun-dong, Dai Yi-qi. Secure two-party computational geometry [J]. Journal of Computer Science and Technology, 2005, 20 (2): 258-263

[9] Luo Yong-long, Huang Liu-sheng, et al. A secure protocol for determining whether a point is inside a convex polygon[J]. Chinese Journal of Electronics, 2006, 15(4): 578-582

[10] 李顺东，戴一奇，王道顺. 几何相交的多方安全保密计算[J]. 清华大学学报：自然科学版，2007，47(10)：1692-1695

[11] 罗永龙，黄刘生. 空间几何对象相对位置判定中的私有信息保护[J]. 计算机研究与发展，2006，43(3)：410-416

[12] Tzeng W. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters [J]. IEEE Trans. on Computers, 2004, 53(2): 232-24

[13] Goldwasser S. Multi-party Computations: Past and Present [D]. Santa Barbara CA: [s. n.], 1997