Secure Two-party Protocols for Point Inclusion Problem

Tony Thomas
Department of Mathematics, Korea Advanced Institute of Science and Technology
Daejeon, 305-701, Republic of Korea. (Email: thomas@knot.kaist.ac.kr)
(Received Nov. 28, 2007; revised and accepted Mar. 3, 2008)

Abstract

It is well known that, in theory, the general secure multiparty computation problem is solvable using circuit evaluation protocols. However, the communication complexity of the resulting protocols depend on the size of the circuit that expresses the functionality to be computed and hence can be impractical. Hence special solutions are needed for specific problems for efficiency reasons. The point inclusion problem in computational geometry is a special multiparty computation and has got many applications. Previous protocols for the secure point inclusion problem are not adequate. In this paper we modify some known solutions to the point inclusion problem in computational geometry to the frame work of secure two-party computation.

Keywords: Computational geometry, multiparty computation, point inclusion problem.

1 Introduction

The rapid growth of networks has opened up tremendous opportunities for cooperative computation, where the output depends on the private inputs of several entities. These computations could even occur between mutually untrusted entities or competitors. The problem is trivial if the context allows to have a trusted entity that would know the inputs from all the participants; however if the context disallows this, then the techniques of secure multi-party computation are used to provide useful solutions.

Generally speaking, a secure multi-party computation problem deals with computing a function in a distributed network where each participant holds one of the inputs, ensuring that no more information is revealed to a participant in the computation than that can be computed from that participant's input and output. The history of the multi-party computation problem is extensive since it was introduced by Yao [25] and extended by Goldreich, Micali, and Wigderson [12] and by many others. These works use a similar methodology: each functionality F is represented as a Boolean circuit, and then the parties run a protocol for every gate in the circuit. The protocols it generates depend on the size of the circuit. This size depends on the size of the input and on the complexity of expressing F as a circuit. If the functionality F is complicated, using the circuit evaluation protocol will typically not be practical. Therefore, Goldreich [11] pointed out that using the solutions from these general results for special cases of multi-party computation could be impractical; special efficient solutions should be developed for specific problems. This is the motivation for seeking solutions to specific cooperative computational problems, in which the solutions are more efficient than the general theoretical solutions. To this end some problems such as comparing two private numbers [14, 17, 26], privacy preserving data mining [1, 18], comparing information [8], privacy preserving geometric computation [5], privacy preserving cooperative scientific computation [4, 13], privacy preserving auction [3], privacy preserving statistical analysis [6, 7], privacy preserving set operations [15] have been investigated.

In secure multi-party computational geometry we seek secure protocols for several geometric problem like point inclusion problem, intersection of two shapes, range searching problem etc where the data is shared by two or more entities. In this paper, we construct secure two-party protocols for the point inclusion problem in star-shaped domains and more complex polygonal domains. Here, one entity Alice has a point M, and Bob has a polygon P. Their aim is to determine whether M is inside P, or not without revealing to each other their private inputs.

We outline the related work in Section 2. In Section 3, we introduce our adversary models as well as the cryptographic tools used in the subsequent sections. In Section 4, we study the point inclusion problem in star-shaped domains and in Section 5, we consider more general polygonal domains. The paper concludes with some remarks in Section 6.

2 Related Work

The secure multiparty computational geometry has got wide applications in the fields of military, computer graphics etc. The study of secure multiparty computational geometry was initiated by Atallah *et al.* [5] with their work on secure point inclusion problem and polygonal intersection problem. Their protocol for the point inclusion problem is applicable to simple polygonal domain and has complexity $O(n)$ where n is the number of edges of the polygon. Later Li *et al.* [16] studied the point inclusion problem for circular domain. However, their solution is not secure in the sense that each party gets additional information regarding the location of the other party's object. Moreover, their solution is highly inefficient. A more efficient protocol for the point inclusion problem in a circular domain was recently proposed by Luo *et al.* [19].

In this paper we consider the point inclusion problem in a star-shaped domain and a more general polygonal domain (can have several disconnected nested components). Two protocols for the star shaped domain with round complexities $O(n)$ and $O(\log n)$ respectively, and a protocols for more general polygonal domain with round complexity $O(n)$, where n is the number of vertices are given.

3 Preliminaries

In this section we state our security assumptions and list the building block for our protocols.

3.1 Security Assumption

We assume that all parties are semihonest. A semi-honest party is the one who follows the protocol correctly with the exception that it keeps a record of all its intermediate computations and might derive the other parties inputs from the record.

The existing protocols listed below serve as important building blocks for our protocols.

3.2 Homomorphic Encryption Schemes

An encryption scheme is homomorphic if for some operations $\oplus$ and $\otimes$, $E_k(x) \otimes E_k(y) = E_k(x \oplus y)$, where x and y are two elements from the message space and k is the key. Many such systems exist, and examples include the systems by Benaloh [2], Naccache and Stern [20], Okamoto and Uchiyama [21], Paillier [22], to mention a few. A useful property of homomorphic encryption schemes is that an addition operation can be conduced based on the encrypted data without decrypting them.

3.3 Yao's Millionaire Protocol

The purpose of this protocol is to compare two private numbers and to determine which one is larger without revealing the numbers. This was first proposed by Yao [25] and is referred as Yao's Millionaire Problem (because two millionaires wish to know who is richer, without revealing any other information about their net wealth). The early cryptographic solution by Yao [25] uses an untrusted third party and has communication complexity that is exponential in the number of bits of the numbers involved. Cachin proposed a solution [3] based on an untrusted third party that can misbehave on its own (for the purpose of illegally obtaining information about Alice's or Bob's private vectors) but does not collude with either participant. The communication complexity of Cachin's scheme is $O(l)$, where l is the number of bits of each input number. Recently many efficient protocols which do not need a third party have been suggested by various authors like [26].

3.4 Scalar Product Protocol

Let Alice has a vector $X = (x_1, \cdots, x_n)$ and Bob has a vector $Y = (y_1, \cdots, y_n)$. The scalar product protocol is to securely compute the scalar (dot) product of X and Y, given by $X.Y = \sum_{k=1}^{n} x_i y_i$.

In [5] Du and Atallah considered a slightly different and more general form of the scalar product protocol in which Alice has the vector X and Bob has the vector Y, and the goal of the protocol is for Alice (but not Bob) to get $X.Y + V$ where V is random and known to Bob only. Their protocols can be easily modified to work for the version of the problem where the random V is given ahead of time as part of Bob's data (the special case $V = 0$ puts us back to the usual scalar product Definition). They had developed two protocols for it. Secure protocols for the scalar product problem can be found in [5, 10, 24].

4 Point Inclusion in Star-shaped Domain

In this section, we study the point inclusion problem in a star-shaped polygonal domain.

Problem: Let Alice has a point M and Bob has a star-shaped polygon P with vertices P_i, for $1 \leq i \leq n$, where the vertices are named in the anticlockwise direction. Alice and Bob want to securely check whether M lies inside (including boundary) P or not.

Since P is a star-shaped polygon, it contains a point Q such the line segments joining Q to P_i for $1 \leq i \leq n$ lies entirely in P. We have the following Algorithm for point inclusion from [23].

Point Inclusion Protocol Without Privacy:

1) Determine by binary search the wedge in which M lies. M lies in the wedge bounded by the rays $\overrightarrow{QP_i}$ and $\overrightarrow{QP_{i+1}}$ if and only if the angle formed by M, Q

and P_i is a left turn and the angle formed by M, Q and P_{i+1} is a right turn.

2) Once P_i and P_{i+1} are found, then M is internal if and only if the angle formed by P_i, P_{i+1} and M is a left turn.

Theorem 1. *[23] The inclusion question can be answered in $O(\log n)$ time, given $O(n)$ space and $O(n)$ processing time.*

To decide whether the angle $\angle P_1P_2P_3$ is a right or left turn corresponds to evaluating a 3×3 determinant in the points' coordinates. Let $P_i = (a_i, b_i)$ for $1 \leq i \leq 3$. The determinant

$$D(P_1, P_2, P_3) = \begin{vmatrix} a_1 & b_1 & 1 \\ a_2 & b_2 & 1 \\ a_3 & b_3 & 1 \end{vmatrix}$$

gives twice the signed area of the triangle $\triangle P_1P_2P_3$, where the sign is + if and only if (P_1, P_2, P_3) forms a counter-clockwise cycle.

Let the coordinates of M be (a, b) and that of Q be (s, t) with respect to some coordinate system known to both Alice and Bob. Now Bob chooses a new coordinate system with origin at Q and axes parallel to the original axes. Let the co-ordinates of P_i with respect to the new coordinate axes be (a_i, b_i) for $1 \leq i \leq n$. The new coordinates of M becomes $(a-s, a-t)$. Now the angle $\angle MQP_i$ is a right turn or left turn according as the determinant

$$D(M, Q, P_i) = \begin{vmatrix} a-s & b-t & 1 \\ 0 & 0 & 1 \\ a_i & b_i & 1 \end{vmatrix}$$

is positive or negative. For $1 \leq i \leq n$, let $A = (a, b, 1)$, $B_i = (-b_i, a_i, sb_i - ta_i)$ and $C_i = ((b_i - b_{i+1}), -(a_i - a_{i+1}), -s(b_i - b_{i+1}) + t(a_i - a_{i+1}) + (a_ib_{i+1} - b_ia_{i+1})$. Now we have,

$$\begin{aligned} D(M, Q, P_i) &= -(a-s)b_i + (b-t)a_i \\ &= -ab_i + ba_i + (sb_i - ta_i) \\ &= (a, b, 1) \cdot (-b_i, a_i, sb_i - ta_i) \\ &= A \cdot B_i. \\ D(P_i, P_{i+1}, M) &= (a-s)(b_i - b_{i+1}) - (b-t)(a_i - a_{i+1}) \\ &\quad +(a_ib_{i+1} - b_ia_{i+1}) \\ &= a(b_i - b_{i+1}) - b(a_i - a_{i+1}) \\ &\quad -s(b_i - b_{i+1}) + t(a_i - a_{i+1}) \\ &\quad +(a_ib_{i+1} - b_ia_{i+1}) \\ &= (a, b, 1).((b_i - b_{i+1}), -(a_i - a_{i+1}), \\ &\quad -s(b_i - b_{i+1}) + t(a_i - a_{i+1}) \\ &\quad +(a_ib_{i+1} - b_ia_{i+1})) \\ &= A \cdot C_i. \end{aligned}$$

The point M lies in the wedge bounded by the rays $\overrightarrow{QP_i}$ and $\overrightarrow{QP_{i+1}}$ if and only if $A.B_i \leq 0$ and $A.B_{i+1} \geq 0$ and if it happens to lie in that wedge, it lies inside the polygon if and only if $A.C_i \leq 0$. Note that Alice has the vector A and Bob has the vectors B_i and C_i for $1 \leq i \leq n$. We now give the corresponding secure protocol for the point inclusion problem.

The Secure Point Inclusion Protocol 4.1:

1) For $i = 1, \cdots, n$, Alice and Bob do the following:
   a. Bob computes B_i, C_i and chooses at random V_i and W_i.
   b. Alice engages in two secure scalar product protocols with Bob and gets $U_i = A.B_i + V_i$ and $Z_i = A.C_i + W_i$.
   c. Alice compares U_i with V_i and Z_i with W_i using millionaire protocol with Bob.
2) Alice identifies the index, $i = j$ at which $U_j < V_j$ and $U_{j+1} > V_{j+1}$.
3) Alice looks at the millionaire protocol output for the pair Z_j and W_j. If Z_j was smaller than W_j then the point is inside else it is outside.
4) Alice communicates the result to Bob.

Analysis of the Protocol 4.1:

Theorem 2. *The Protocol 4.1 is correct, secure and has round complexity $O(n)$.*

Proof.
Correctness: Using the millionaire protocol, in Step 2 Alice identifies the wedge in which the point M lies and in Step 3 she checks whether the point M lies inside or outside the polygon. The correctness of the protocol follows from the correctness of the corresponding insecure protocol.

Security: The security of the protocol immediately follows from the privacy of the secure scalar product protocol and that of the secure protocol for the millionaire problem. Also, Alice does not reveal to Bob the wedge in which M lies, and so Bob will not get any idea about the location of the point M.

Round Complexity: It is easy to see that the round complexity of the protocol is $O(n)$. □

Binary Search to Reduce Round Complexity:

Now, we will incorporate binary search in the above protocol to reduce its round complexity to $O(\log n)$. A binary search Algorithm is a technique for finding a particular value in a sorted list. It searches a sorted array by repeatedly dividing the search interval into half. Begin with an interval covering the whole array. If the value of the search key is less than the item in the middle of the interval, narrow the interval to the lower half.

Otherwise narrow it to the upper half. Repeatedly check until the value is found or the interval is empty. Clearly the complexity of this search Algorithm is $O(\log n)$, where n is the size of the sorted list.

Let E be a homomorphic commutative encryption scheme. That is if (E_A, D_A) and (E_B, D_B) be the encryption and decryption pairs of Alice and Bob corresponding to their keys and let $E = E_A$ or E_B, then

1) $E_A(E_B(x)) = E_B(E_A(x))$;
2) $E(x) * E(y) = E(x.y)$.

Given $U = (u_1, \cdots, u_n)$, let $E(U) = (E(u_1), \cdots, E(u_n))$. We now give the modified secure protocol for the point inclusion problem.

The Secure Point Inclusion Protocol 4.2:

1) For $1 \leq i \leq n$, Bob computes $b_i = E_B(B_i)$, and $c_i = E_B(C_i)$.
2) Bob sends $(b_1, \cdots, b_n)$ and $(c_1, \cdots, c_n)$ to Alice.
3) Alice picks an r randomly such that $1 < r < n$ and cyclically rotates the lists obtained from Bob by r positions to get $(b_{1+r}, \cdots, b_r)$ and $(c_{1+r}, \cdots, c_r)$.
4) Alice sends $(E_A(b_{1+r}), \cdots, E_A(b_r))$ and $(E_A(c_{1+r}), \cdots, E_A(c_r))$ to Bob.
5) Bob decrypts the list obtained from Alice with his private key D_B and obtains

$$\begin{aligned} & (D_B(E_A(b_{1+r})), \cdots, D_B(E_A(b_r))) \\ = \; & (E_A(B_{1+r}), \cdots, E_A(B_r)), \end{aligned}$$

and

$$\begin{aligned} & (D_B(E_A(c_{1+r})), \cdots, D_B(E_A(c_r))) \\ = \; & (E_A(C_{1+r}), \cdots, E_A(C_r)). \end{aligned}$$

6) Alice computes $E_A(A)$.
7) Alice identifies the index, $i = j$ for which $A.B_j < 0$ and $A.B_{j+1} > 0$ using the following sub protocol in the binary search.
   a. For each index k Alice picks up in the binary search, Bob picks a random $r_k > 0$ encrypts with his key and sends Alice $E_B(r_k)$.
   b. Alice encrypts with her key and sends back to Bob $E_A(E_B(r_k))$.
   c. Bob decrypts and obtains $D_B(E_A(E_B(r_k))) = E_A(r_k)$.
   d. Bob computes $E_A(r_k) * E_A(B_k) = E_A(r_k B_k)$.
   e. Alice engages in a secure scalar product protocol with Bob and obtains $E_A(A) * E_A(r_k B_k) = E_A(r_k(A.B_k))$.
   f. Alice decrypts and obtains $D_A(E_A(r_k(A.B_k)) = r_k(A.B_k)$ and checks whether it is positive or not.
8) Alice checks whether $A.D_j$ is negative or positive using a similar sub protocol as in Step 7. If it is negative, the point is inside else it is outside.
9) Alice communicates the result to Bob.

Analysis of the Protocol 4.2:

Theorem 3. *The Protocol 4.2 is correct, secure and has round complexity $O(\log n)$.*

Proof.
Correctness: It is clear that, in Step 5, Bob gets the encryption of the vectors B_i and C_i for $1 \leq i \leq n$ with the key of Alice. For each index k occurring in the binary search, Alice has $E_A(A)$ and Bob has $E_A(r_k B_k)$. Using the secure scalar product protocol she obtains $E_A(A) * E_A(r_k B_k)$, which is equal to $E_A(r_k A.B_k)$ from the homomorphic property of the encryption scheme. By decryption using her private key Alice gets $r_k(A.B_k)$ and she can check whether $A.B_k \geq 0$, since $r_k > 0$. Thus Alice can identify the wedge in which the point M lies. Similarly, once the wedge is identified, she can check whether the point lies inside the polygon or not. Thus the correctness of the protocol follows from the correctness of the corresponding insecure protocol.

Security: Since Bob is sending B_i and C_i for $1 \leq i \leq n$, after encryption with his key, Alice will not get any information about the private data of Bob. Since Alice rotates the list of B_i and C_i after masking with her key, Bob will not get any idea of the specific B_i and C_i Alice is using in the binary search in Step 7. Hence, Bob will not get any idea of the wedge in which the point M lies. The privacy of the secure scalar product protocol guarantees the privacy of the individual inputs during the scalar product computation in Step 7 and Step 8. Also since r_k is random known only to Bob, the only information Alice can get from the scalar product is its sign.

Round Complexity: As Alice is using binary search in the identification of the wedge in which the point M lies, it is clear that the round complexity of the protocol is $O(\log n)$, since the complexity of the binary search is $O(\log n)$. □

5 Point Inclusion in More General Polygonal Domain

In this section, we consider an Algorithm for the point inclusion problem for a more general polygonal domain given in [9]. This domain is more general than any of the domains so far considered in the context of secure point inclusion problem.

Problem: Alice has a point M and Bob has a polygon P that may have multiple disconnected nested components,

with vertices $P_1, \cdots, P_n$. Alice and Bob wants to securely check whether M lies inside (including boundary) P or not.

The *characteristic function*, $\chi(M)$ of the polygon P is defined as,

$$\chi(M) = \begin{cases} 1 & \text{if } M \text{ lies on or inside } P; \\ 0 & \text{otherwise,} \end{cases}$$

where $M \in \mathbb{R}^2$. Let $0 < \theta < 2\pi$, be the included angle (edges swept inside the polygon) at a vertex V. The extension to ∞ in both directions of the edges incident on the vertex V divide the plane into 4 wedges. If $\theta < \pi$ (convex vertex), there are two wedges with angle θ and two wedges with angle $\pi - \theta$. We call the wedges with angle θ as inner and those with angle $\pi - \theta$ as outer. If $\theta > \pi$ (concave vertex), there are two wedges with angle $2\pi - \theta$ and two wedges with angle $\theta - \pi$. In this case, we call the wedges with angle $2\pi - \theta$ as inner and those with angle $\theta - \pi$ as outer.

We assume for convenience that the point M does not lie on any of the four rays emanating from any of the vertices of the polygon. The case in which M lies on a ray can be easily handled separately. Now, the *cross function*, $\rho_V(M)$ of a point M with respect to a vertex V of the polygon is defined as

$$\rho_V(M) = \begin{cases} \frac{1}{2} - \frac{\theta}{2\pi} & \text{if } \theta < \pi \text{ and } M \text{ is in an inner wedge;} \\ -\frac{\theta}{2\pi} & \text{if } \theta < \pi \text{ and } M \text{ is in an outer wedge;} \\ \frac{\theta}{2\pi} - \frac{1}{2} & \text{if } \theta > \pi \text{ and } M \text{ is in an inner wedge;} \\ \frac{\theta}{2\pi} & \text{if } \theta > \pi \text{ and } M \text{ is in an outer wedge.} \end{cases}$$

Theorem 4. *[9] The characteristic function of the whole polygon is the sum of the cross functions of its vertices. That is*

$$\chi(M) = \sum_{V=P_1}^{P_n} \rho_V(M), \qquad \forall M \in \mathbb{R}^2.$$

Before we give the secure protocol for the point inclusion problem, we outline a way for Alice to securely identify whether her point lies in an inner or outer wedge corresponding to a vertex V. Bob chooses four points V_1, V_2, V_3 and V_4 on the four rays emanating from the vertex V. Without loss of generality let us suppose that $\overrightarrow{VV_1}$ and $\overrightarrow{VV_2}$ bound one inner wedge and $\overrightarrow{VV_3}$ and $\overrightarrow{VV_4}$ bound the other one. Now Alice and Bob engages in a secure protocol (as described in the previous section) and Alice checks whether M is inside any of these two wedges. If that is the cases M is inside an inner wedge else M is inside an outer wedge.

For $1 \leq i \leq n$, let θ_i be the included angle at the vertex P_i. We now give a secure protocol for the point inclusion problem.

The Secure Point Inclusion Protocol 5.1:

1) Bob computes $\theta = \sum_{i=1}^{n} (-1)^{m_i} \frac{\theta_i}{2\pi}$, where $m_i = 0$ if V_i is a convex vertex ($\theta_i < \pi$) and $m_i = 1$, otherwise.
2) For $1 \leq i \leq n$ Alice and Bob do the following.
   a. For the vertex V_i, Alice checks whether M lies inside an inner or outer wedge using the protocol described above.
   b. If the wedge is inner, Alice assigns $u_i = \frac{1}{2}$, else she assigns $u_i = 0$.
   c. If the edge is convex Bob assigns $v_i = 1$, else he assigns $v_i = -1$.
3) Alice assigns $U = (u_1, \cdots, u_n)$.
4) Bob assigns $V = (v_1, \cdots, v_n)$.
5) Bob engages in a secure scalar product protocol with Alice and gets $U.V$.
6) Bob computes $\chi(M) = U.V + \theta$.
7) Bob communicates the result to Alice.

5.1 Analysis of the Protocol 5.1

Theorem 5. *The Protocol 5.1 is correct, secure and has round complexity $O(n)$.*

Proof.
Correctness: Let E_1 be the set of convex vertices where the point M lies in an inner wedge, E_2 be the set of convex vertices where the point M lies in an outer wedge, E_3 be the set of concave vertices where the point M lies in an inner wedge and E_4 be the set of concave vertices where the point M lies in an outer wedge. Then we have,

$$\begin{aligned} \chi(M) &= \sum_{V=P_1}^{P_n} \rho_V(M) \\ &= \sum_{V_i \in E_1} \rho_{V_i}(M) + \sum_{V_i \in E_2} \rho_{V_i}(M) + \sum_{V_i \in E_3} \rho_{V_i}(M) \\ &\quad + \sum_{V_i \in E_4} \rho_{V_i}(M) \\ &= \sum_{V_i \in E_1} \frac{1}{2} - \frac{\theta_i}{2\pi} + \sum_{V_i \in E_2} -\frac{\theta_i}{2\pi} + \sum_{V_i \in E_1} \frac{\theta_i}{2\pi} - \frac{1}{2} \\ &\quad + \sum_{V_i \in E_1} \frac{\theta_i}{2\pi} \\ &= \sum_{i=1}^{n} (-1)^{m_i} \frac{\theta_i}{2\pi} + U.V. \end{aligned}$$

Thus Bob can compute $\chi(M)$ and hence the protocol is correct.

Security: The security of the protocol immediately follows from the privacy of the secure scalar product protocol and that of the secure protocol for the millionaire

problem.

Round Complexity: It is clear that the round complexity of the protocol is $O(n)$. □

6 Conclusion

In this paper, we studied the secure point inclusion problem for polygonal domains in a plane in the presence of passive adversaries. The existing secure protocols for the point inclusion problem in general polygonal domains have a round complexity of $O(n)$, where n is the number of edges of the polygon. In Section 4, we exploited the special structure of the star shaped domains and used the binary search Algorithm to reduce the round complexity to $O(\log n)$ in Protocol 4.2. The secure protocols for the point inclusion problem so far have been proposed only for simple polygonal domains and for circular domains. In Section 5, we tried to extend the study to more complex domains. The Protocol 5.1 for the general polygonal domains is applicable for a large class of polygonal domains than the existing protocols.

As a direction for future research, it will be interesting to extend these ideas to more general domains in a plane and to higher dimensional spaces. It is worth mentioning that analogous to Theorem 5.1 can be found in dimension three. A bigger challenge in front of us is to build secure protocols which are very efficient in terms of round as well as computational complexity in the presence of active adversaries for the point inclusion problem and the range searching problem for arbitrary domains in dimensions two, three and even higher.

Acknowledgments

This work was carried out while the author was a postdoctoral researcher at KAIST, Korea. The author is grateful to Prof. Ki Hyoung Ko for the helpful discussions with him and the anonymous reviewers for their valuable comments.

References

[1] R. Agrawal, and R. Srikant, "Privacy preserving data mining," *Proceedings of the ACM SIGMOND on Management of Data*, pp. 439-450, ACM Press, 2000.

[2] J. Benaloh, "Dense probabilistic encryption," *Proceedings of the Workshop on Selected Areas of Cryptography*, pp. 120-128, Kingston, ON, May 1994.

[3] C. Cachin, "Efficient private bidding and auctions with an oblivious third party," *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pp. 120-127, Singapore, Nov. 1-4, 1999.

[4] W. Du, and M. J. Atallah, "Privacy-preserving cooperative scientific computations," *14th IEEE Computer Security Foundations Workshop*, Nova Scotia, Canada, Jun. 11-13, 2001.

[5] W. Du, and M. J. Atallah, "Secure multiparty computational geometry," *Algorithms and Data Structures : 7th International Workshop, WADS*, Providence, RI, USA, Aug. 8-10, 2001.

[6] W. Du, and M. J. Atallah, "Privacy-preserving cooperative statistical analysis," *Proceedings of the 17th Annual Computer Security Applications Conference*, pp. 102-110, New Orleans, USA, Dec. 10-14, 2001.

[7] W. Du, Y. S. Han, and S. Chen, "Privacy-preserving multivariate statistical analysis: Linear regression and classification," *Proceedings of SIAM Int Conference Data Mining (SDM)*, Apr. 2004.

[8] R. Fagin, M. Naor and P. Winkler, "Comparing information without leaking it," *Communication of the ACM*, vol. 39, pp. 77-85, 1996.

[9] W. R. Franklin, "Polygon properties calculated from the vertex neighborhoods," *Annual Symposium on Computational Geometry, Proceedings of the third Annual Symposium on Computational Geometry*, pp. 110-118, Waterloo, Ontario, Canada, 1987.

[10] B. Goethals, S. Laur, H. Lipmaa, and T. Mielikainen, "On Private Scalar Product Computation for Privacy-Preserving Data Mining," in *The 7th Annual International Conference in Information Security and Cryptology (ICISC)*, LNCS 3506, pp. 104-120, Springer-Verlag, Seoul, Korea, Dec. 2-3, 2004.

[11] O. Goldreich, *Secure Multi-party Computation (Working Draft)*, 1998. (http://citeseer.ist.psu.edu/goldreich98secure.html)

[12] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," *Proceedings of the 19th Annual ACM Conference on Theory of Computing*, pp. 218-229, New York, 1987.

[13] S. Goldwasser, and Y. Lindell, "Secure comptutation without agreement," *Proceedings of 16th DISC*, LNCS 2508, pp. 17-32, 2002.

[14] I. Ioannidis, and A. Grama, "An efficient protocol for Yao's millionaires' problem," *Proceedings of the 36th Hawaii International Conference on System Sciences*, Jan. 6-9, 2003.

[15] L. Kissner, and D. Song, "Privacy preserving set operations," *Advances in Cryptology: Crypto*, LNCS 3621, pp. 241-257, 2005.

[16] S. D. Li, and Y. Q. Dai, "Secure two-party computational geometry," *Journal of Computer Science and Technology*, vol. 20, no. 2, pp.258-263, 2005.

[17] H. Y. Lin, and W. G. Tzeng, "An efficient solution to the millionaires' problem based on hormomorphic encryption," *Applied Cryptography and Network Security*, LNCS 3531, pp. 456-466, Springer-Verlag, 2005.

[18] Y. Lindell, and B. Pinkas, "Privacy preserving data mining," in *Journal of Cryptology*, vol. 15, no. 3, pp. 177-206, 2002.

[19] Y. L. Luo, L. S. Huang, and H Zhong, "Secure two-party point-circle inclusion problem," *Journal of Computer Science and Technology*, vol. 22, no. 1, pp.88-91, 2007.

[20] D. Naccache, and J. Stern, "A new cryptosystem based on higher residues," *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pp. 59-66, 1998.

[21] T. Okamoto, and S. Uchiyama, "An efficient public-key cryptosystem," *Advances in Cryptology, Eurocrypt '98*, pp. 308-318, 1998.

[22] P. Paillier, "Public-key cryptosystems based on composite degree residue classes," *Advances in Cryptology, Eurocrypt '99*, LNCS 1592, pp. 223-238, 1999.

[23] F. P. Preparata, and M. I. Shamos, *Computational Geometry An Introduction*, Chapter 2, Section 2.2, Springer.

[24] Z. Yang, R. N. Wright, and H. Subramaniam, "Experimental analysis of a privacy-preserving scalar product protocol," *International Journal of Computer Systems Science and Engineering*, vol. 21, no. 1, pp. 47-52, 2006.

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

[26] L. Yonglong, and H. Liusheng, "An efficient private comparison problem," Preprint.

Tony Thomas received his M.Sc and Ph.D. degrees in Mathematics from IIT Kanpur, India in 1998 and 2006 respectively. He was a Postdoctoral Researcher in the Department of Mathematics, KAIST, Korea from August 2006 to July 2007. Currently he is working as a researcher in the Vehicular Communications Research Group, General Motors Technical Center, Bangalore India. His research interests include public-key cryptography, secure multiparty computations, security in wireless ad-hoc networks.