ARTICLE IN PRESS

Information Sciences xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Secure multiparty computation of solid geometric problems and their applications ☆

Shundong Li [a,*], Chunying Wu [a], Daoshun Wang [b], Yiqi Dai [b]

[a] School of Computer Science, Shaanxi Normal University, Xi'an 710062, China
[b] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

ARTICLE INFO

Article history:
Received 8 August 2009
Received in revised form 31 October 2012
Accepted 9 April 2014
Available online xxxx

Keywords:
Cryptography
Secure multiparty computation
Solid geometry
Protocol
Simulation paradigm

ABSTRACT

Secure multiparty computation is an area of recent research in the international cryptographic community, and secure computational geometry is an essential field of secure multiparty computation. Most of the existing studies of secure multiparty computational geometric problems have focused on plane geometry, while very few have addressed solid geometry. Because solid geometry is an integral part of geometry and describes the real world better than plane geometry, research on secure computational solid geometry is appealing. Motivated by an interesting application, we first examine the problem of the secure multiparty computation of a tetrahedron, propose a solution, and prove that the solution is private using an accepted simulation paradigm. Using the solution to the tetrahedron problem as a building block, we further solve the secure multiparty computation of three other solid geometric problems, including the relationship between a point and a plane, the relationship between a line and a plane, and the relationship between two planes. We also demonstrate that the solutions to these problems are private. We analyze the computational and communication complexities of these solutions and show that the computational complexities are near or equal to the problems' minimum theoretical computational complexity and that the communication complexities are equal to the minimum theoretical communication complexity. Thus, these solutions are optimal. Finally, we show an interesting application of secure computational solid geometry.

1. Introduction

Secure multiparty computation is the generalization of Yao's millionaires problem [1]. It is the general form of several types of cryptographic protocols, including key agreement protocols [2,3], digital signature protocols, zero-knowledge proof protocols, secret sharing protocols [4], and oblivious transfer protocols [5]. Secure multiparty computation has many applications in cryptography and the virtual world. It is a crucial technology that is used to preserve data privacy in networks, in data mining [6], and in electronic commerce [7]. The many applications of secure multiparty computation have made it a research focus in the international cryptographic community. Goldwasser [8] predicted that secure multiparty computation,

☆ Project Supported by the National Natural Science Foundation of China (Grant Nos. 61070189, 61272435, and 61373020) and National High Technology Development (863) Program (2008AA01Z419).

* Corresponding author. Tel.: +86 29 85310161; fax: +86 29 85310161.
E-mail address: shundong@snnu.edu.cn (S. Li).

http://dx.doi.org/10.1016/j.ins.2014.04.004
0020-0255/

which is a powerful tool and has a rich theoretical basis but whose real-life usage is only beginning, will become an integral part of our computing reality in the future.

Goldreich et al. [5,9] studied the theoretical problems of secure multiparty computation. Goldreich's work laid the theoretical basis for secure multiparty computation; he proved that secure multiparty computation problems are theoretically solvable, and he established a simulation paradigm that has been extensively used to evaluate whether a multiparty computation protocol is secure. Goldreich [5] also designed an important compiler. Given a protocol π that privately computes a function f in a semi-honest model, his compiler can produce a new protocol Π that can privately compute f in the malicious model. This work is important because it demonstrates that any secure multiparty computation problem can be solved with his universal method, although the solution may be inefficient. In addition, his work suggests that the method is sufficient to study the solutions to any secure multiparty computation problems in the semi-honest model.

The conclusion that the general secure multiparty computation problems are theoretically solvable does not mean that they are solvable in practice. Theoretical solvability does not consider the time needed to solve a problem; solving a theoretically solvable problem may take hundreds of years or more. Practical solvability requires a polynomial time algorithm, but no work has provided such an algorithm for the general secure multiparty computation problem. Goldreich [5] further notes that the solutions derived by these general results can be impractical in special cases; therefore, efficient solutions should be developed in special cases.

Motivated by Goldwasser's predictions and Goldreich's observations, cryptographic researchers have studied many types of secure multiparty computation problems as well as their efficient solutions. Secure multiparty computational geometry is one of several types of secure multiparty computation problems. Applications of secure multiparty computational geometry have been studied extensively [10,11]. Du [12,13] studied and proposed solutions to the point inclusion problem, the problem of the intersection of two line segments, the problem of the intersection of two polygons, and the convex hull problem for a set of private points. Other secure multiparty computational geometric problems that have been studied include the distance between two private points, the intersection of two circles or ellipses [14], geometric inclusion problems [15,16], spatial position relationships [17], the closest pair in two dimensional space [18], polygon intersections [19], planar circles [20], and point-curve relationships [21].

Although several studies have focused on secure multiparty computational geometry, additional problems need to be studied more extensively, especially problems with strong applications. At present, all studies of secure multiparty computational geometry have focused on plane geometry problems and have largely ignored solid geometric problems. Both plane geometry and solid geometry are essential areas of geometry. Solid geometry can better depict the real world, so research on problems in solid geometry are appealing.

Secure multiparty computational solid geometry has extensive practical applications. In this paper, we show an interesting direct application of our protocol, which appears at first glance to have no relation to computational geometry but is closely related to plane and solid computational geometry. The plane computational geometric case has been investigated, though the application is not described; in this paper, we study the secure computation of the solid case of this problem. We design a protocol to solve this problem directly. For details, please see the application section.

An example of a problem in secure computational solid geometry is one in which the military needs to establish a secret base in a particular area. The base must have a reliable water supply in the area; however, the Department of Geology and Mineral Resources, rather than the military, knows the distribution of the groundwater resource. The military cannot tell the Department of Geology and Mineral Resources where it wants to establish the base, and the Department of Geology and Mineral Resources is unwilling to give the military information on the distribution of the groundwater resource. How can the military determine if there is a reliable groundwater resource? The solution to this problem requires secure multiparty computation technology in the form of secure multiparty computational solid geometry. Thus, the importance of solid geometry calls for research into secure multiparty computational solid geometry.

1.1. Our contributions

The main contributions of this study are as follows:

(1) Exploring the application of secure multiparty computation is an important aspect of secure multiparty computation research. In this paper, we first show an interesting application of secure multiparty computation in the oil and chemical industry. This application is closely related to secure computational geometry.
(2) To solve the problem proposed in (1), we then study the secure multiparty computation of the volume of a tetrahedron, propose its solution, and prove the privacy-preserving property of this solution using a simulation paradigm.
(3) Based on the secure multiparty computation solution for the volume of a tetrahedron, we solve the following three secure multiparty computational solid geometric problems and propose corresponding solutions:
    (i) The relationship between a point and a plane. The protocol for this problem can be used to solve the application that we describe in this paper.
    (ii) The relationship between a line and a plane.
    (iii) The relationship between two planes.

Please cite this article in press as: L. Shundong et al., Secure multiparty computation of solid geometric problems and their applications, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.04.004