Journal of Network and Computer Applications 46 (2014) 94–99

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A new Lagrange solution to the privacy-preserving general geometric intersection problem

Jing Qin [a,*], Hongwei Duan [a,b], Huawei Zhao [c], Jiankun Hu [a,d]

[a] School of Mathematics, Shandong University, Jinan, China
[b] Experimental School Attached to Haidian Teachers Training College, Beijing, China
[c] School of Computer & Information Engineering, Shandong University of Finance & Economics, Jinan, China
[d] School of Engineering and Information Technology, University of New South Wales, Canberra, Australia

ARTICLE INFO

Article history:
Received 28 May 2013
Received in revised form
15 May 2014
Accepted 10 August 2014
Available online 27 August 2014

Keywords:
Intersection problem
Judging private path problem
Privacy-preserving computational geometry
Lagrange multiplier method
Security

ABSTRACT

Secure multi-party computation (SMC) is an important problem in cryptography. Existing solutions are mostly based on circuit evaluation protocols which are impractical. In this paper, a solution is proposed by abstracting the intersection problem and the judging private path problem into a general intersection problem, i.e., if two participants have a private curve and do not disclose their private curve data, how to solve two-free-plane–curve intersection problem in a cooperative environment. A systematic Lagrange multiplier method is proposed to combat the general intersection problem instead of focusing on normal curves case. The proposed systematic method can systematically deal with various intersection problems faced in practical applications. In addition, the proposed method can also solve the normal curves cases.

1. Introduction

Secure multi-party computation (SMC) has recently become a research focus in the international cryptographic community. It was first introduced by Yao (1982), and general results concerning secure two-party and multi-party computations were introduced by Goldreich et al. (1987), Goldreich (2002, 2004). SMC has attracted a strong interest as soon as it was introduced (Yao, 1982; Goldreich et al., 1987; Goldreich, 2002, 2004; Fischlin, 2001; Bo et al., 2005; Du, 2001; Qin et al., 2004a, 2004b; Huang et al., 2013; Mohassel and Riva, 2013; Asharov, 2014; Kiyoshima et al., 2014; Hazay and Patra, 2014). It should be emphasized that if we can compute any function securely, then we will have a very powerful tool, virtually all natural protocol problems can be rephrased to be special cases of the multi-party computation problem (Goldreich, 2002; Goldwasser, 1997).

Generally speaking, SMC problem deals with computing a function on any input 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 what can be computed from that participant's input and output. It is well known that, in theory, the general SMC problem is solvable using circuit evaluation protocols (Goldreich et al., 1987; Goldreich, 2002). However, as Goldreich (2002) pointed out, using the solutions derived from these general results to solve specific problems can be impractical. Problem-specific solutions should be developed, for efficiency reasons. In fact, design and analysis of the special two-party or multi-party computation protocols is meaningful and it has attracted much interest in this field (Fischlin, 2001; Bo et al., 2005; Du, 2001; Qin et al., 2004a, 2004b; Mohassel and Riva, 2013; Asharov, 2014; Kiyoshima et al., 2014; Hazay and Patra, 2014).

Privacy-preserving computational geometry is a special SMC problem. Privacy-preserving computational geometry problem refers to that two participants need to solve a geometric problem based on their joint data, but neither wants to disclose their private data to the other participant. It has many applications. For secure multi-party geometry computation, the following two scenarios describe some potential applications that are related to this problem:

Scenario 1: Country A decides to bomb a location x in another country. However, A does not want to hurt its relationship with its friends, who might have some areas of interests in the bombing region. For example, those countries might have secret businesses, secret military bases, or secret agencies in that area. Obviously, A does not want to disclose the exact location of x to all of its friends, except the one who will definitely be hurt by this bombing. On the other hand, its friends do not want to disclose their secret areas to A either,

[*] Corresponding author.
E-mail addresses: qinjing@sdu.edu.cn (J. Qin), hwduansdu@163.com (H. Duan), zhuav@163.com (H. Zhao), J.Hu@adfa.edu.au (J. Hu).

http://dx.doi.org/10.1016/j.jnca.2014.08.004

unless they are in the target area. How could they solve this dilemma? If each secret area is represented by a secret polygon, the problem becomes how to decide whether A's secret point is within B's polygon, where B represents some of the friendly countries. If the point is not within the polygon, no information should be disclosed including the information such as whether the location is at the west of the polygon, or within certain longitude or latitude. Basically, it is “all-or-nothing”: if one will be bombed, it knows all; otherwise it knows nothing.

Scenario 2: In the process of making virtual military command system, attackers want to secretly go through the region where is defended by guards. Both attackers and guards want to know whether the attackers' path intersects with the region, without revealing attackers' military intention and guards' firepower arrangement. Also, they refrain from involving the third party in the determination process. This problem is referred as judging private path problem. Judging private path is a kind of special privacy-preserving computational geometry problem.

This paper will present a new systematic method to solve the secure two-part computational geometry. Our contributions are summarized as follows:

(i) We extend the judging private path problem to the general case, i.e., free plane geometry regions instead of restricted ellipse area and present a new systematic method to solve the secure two-part computational geometry without using Secure Two-Party Scalar Product Protocol and Secure Two-Party Vector Dominance Protocol which are considered as the two building blocks in the previous works. This will greatly improve the accuracy and efficiency.

(ii) Most researchers usually use polygons to approximate the curve in order to cope with the abnormal curves. Obviously polygons as segment liner functions can be used to approximate the curve, but unfortunately such linear approximation functions are far from fine-grain which leads to large approximation errors. We will use both segment linear functions and quadratic curves to approximate the border of a region in order to improve curve approximation accuracy.

(iii) We have used the Bezier curves, Bernstein curves and *B* spline curves to improve the approximation accuracy of the free curves.

(iv) We propose a systematic solution based on the Lagrange multiplier method to determine whether two free curves intersect. This is different from the traditional methods that are based on the two building blocks in the field.

The proposed scheme will transfer the geometry computation problems to algebraic computation problems which can be solved efficiently by many existing advanced methods. The remaining organization of the paper is as follows. Section 2 is for related work. Section 3 will provide some preliminaries necessary for the understating of our proposed schemes. The proposed systematic method will be illustrated in Section 4. Section 5 will be devoted to conclusions and future work.

2. Related works

Atallah and Du (2001) considered several secure two-party computational geometry problems, such as point-inclusion problem, intersection problem, and closest pair problem, etc. Meanwhile, they had presented two preliminary works for solving such problems. These were Secure Two-Party Scalar Product Protocol and Secure Two-Party Vector Dominance Protocol. In computational geometry field, these two building blocks and Yao's Millionaire Protocol have become benchmark modules which are widely used. The complexity of the these protocols in solving the computational geometry problems depends on the size of the circuit, the two building blocks and Yao's Millionaire Problem.

Point-inclusion problem and intersection problem are of the cornerstone of the privacy-preserving computational geometry. In fact, point-inclusion problem can be considered as a simplified case of the intersection problem, and the solutions to the intersection problem can be applied to the point-inclusion problem. Du (2001) used the two basic building blocks for solving such problems. Li et al. (2005) used Monte Carlo method to compute arbitrary geometric region's area and utilized Cantor code to investigate whether or not two arbitrary geometric regions intersect. Then they gave an approximate protocol. Although they were the first methods used in dealing with arbitrary geometric regions' intersection problem, Monte Carlo method is a probabilistic method, which will inevitably lead to errors. Accordingly, the stability of Monte Carlo method would affect the determined outcome and may cause misleading results.

Judging private path problem is an essential problem in practical applications. Fu et al. (2010) have investigated some simplified special cases e.g. the relation between a private point and an ellipse area, a line or a segment line and an ellipse area. They gave a point inclusion an ellipse area protocol. In terms of a line or a segment line, they dispersed a line to a point collection with a minimal value. Subsequently, they utilized a point inclusion an ellipse area protocol to determine whether or not a line or a segment line and an ellipse area intersect. Dong and Jia (2009) have introduced the work of digital curve approximation by polygons and systematically summarized various methods of digital curve approximation by polygons. Andre and Odemir (2013) comprehensively elaborated the polygonal approximation of digital planar curves theory from the point of view of information sciences. Recent research works (Huang et al., 2013; Mohassel and Riva, 2013; Asharov, 2014; Kiyoshima et al., 2014; Hazay and Patra, 2014) focus on special two-party or multi-party computation protocols in order to improve their efficiency and security. However the issue of privacy-preserving computational geometry has not been considered which will be addressed in this paper.

3. Preliminaries

In this section, we provide some necessary notations, definitions, and known results that will be used throughout the paper.

3.1. Security assumption

Our work assumes that all participants are semi-honest. Roughly speaking, a semi-honest party is the one who follows the protocol properly with the exception that it keeps a record of all its intermediate computations and might try to derive other participants' private inputs from the record.

3.2. Problem 1 (point-inclusion)

Alice has a point s, and Bob has a polygon P. They want to determine whether z is inside P without revealing to each other anything more than what can be inferred from that answer. In particular, neither of them is allowed to learn such information about the relative position of z and P as whether z is at the northwest side of P, or whether z is closer to one of the borders of P, etc.