




# Method and Application of Homomorphic Subtraction of the Paillier Cryptosystem in Secure Multi-party Computational Geometry

Meng Liu<sup>1</sup>(✉) , Yun Luo<sup>2</sup>, Chi Yang<sup>3</sup>, Dongliang Xu<sup>1</sup>, and Taoran Wu<sup>4</sup>

<sup>1</sup> School of Mechanical, Electrical and Information Engineering,  
Shandong University, Weihai, China  
{liumeng,xudongliang}@sdu.edu.cn

<sup>2</sup> Faculty of Engineering and Information Technology,  
University of Technology Sydney, Ultimo, Australia  
yun.luo@student.uts.edu.au

<sup>3</sup> School of Computer Science and Technology, Huazhong University of Science  
and Technology, Wuhan, China  
chiyangit@gmail.com

<sup>4</sup> College of Professional Studies, Northeastern University, Boston, USA  
wu.ta@husky.neu.edu

**Abstract.** A secure two-party computation protocol for the problem of the distance between two private points is important and can be used as the building block for some secure multi-party computation (SMC) problems in the field of geometry. Li's solution to this problem is inefficient based on  $OT_m^1$  oblivious transfer protocol and some drawbacks still remain while applied to compute the relationship between a private circle and a private point. Two protocols are also proposed based on the Paillier cryptosystem by Luo et al. and more efficient than Li's solution, but there also remain some drawbacks. In this paper, we propose an idea to improve the efficiency of secure protocol by using its homomorphic subtraction based on the Paillier cryptosystem. Then we apply it to solve the secure two-party computation problem for the distance between two private points. Using our solution, the SMC protocol to the relationship between a private point and a private circle area is more efficient and private than Li's solution. In addition, we also find that our solution is also more efficient than the BGN-based solution and much better while the plaintext can be in some large range.

**Keywords:** Secure multi-party computation · Homomorphic cryptosystem · Computational geometry · Subtraction

---

Supported by Shandong Provincial Natural Science Foundation under grant ZR2019PF007.

## 1 Introduction

SMC protocol can be employed for collaboratively computing a function by parties based on multiple private input information, but these private inputs will not be revealed. SMC is a very important research area in cryptographic research problems, and its solutions have been widely used in secure statistical analysis [11], privacy-preserving clustering [16], data mining [1, 18], bidding and auction [7, 26], cooperative scientific computation [10, 28], set intersection [9, 12, 27] and secure computational geometry [2, 6, 19, 29, 30]. Yao's Millionaires' problem is the first SMC problem that was introduced by Yao [20, 31].

The secure calculation of the distance between two private points is a fundamental problem that needs to be solved in the field of geometry and an SMC protocol to it can be used as a building block for some SMC geometry problems [17, 20]. Secure multi-party computational geometry problem is a special area of SMC, and we should put forward to some special solutions to these problems that are more effective than general theoretical solutions.

The rest of this paper is organized as follows:

We outline the related work in Sect. 2. In Sect. 3, we introduce and demonstrate a method of homomorphic subtraction of the Paillier cryptosystem. We apply our method to solve the secure two-party computation problem for the distance between two private points in Sect. 4. In Sect. 5, an SMC protocol to the relationship between a private circle area and a private point is proposed by using our protocol in Sect. 4. In Sect. 6, we show efficiency analysis and experiment results between our solution and Li's solution. And we also compare and analyse the computation costs of the solutions based on the Paillier cryptosystem and the BGN cryptosystem. The last section concludes this paper and discusses the future work.

## 2 Related Work

Some computational geometry problems have been studied [2, 17]. However, most of their solutions are based on  $OT_m^1$  oblivious transfer protocol. These solutions need so many oblivious transfer that they are not very efficient. Li et al. [17] researched the secure two-party computation problem for the distance between two private points based on  $OT_m^1$  protocol, but their solution is highly inefficient. While Protocol 2 proposed in [17] is applied to compute the relationship between a private point and a private circle, there are still some drawbacks. Homomorphic Cryptosystem is used more and more in SMC fields, especially Millionaire protocol. The Paillier cryptosystem supports additively homomorphic encryption and has been widely used in some solutions to secure multi-party computation. Luo et al. [22] present a protocol for solving the problem of secure computation for the distance between two private points based on the Paillier cryptosystem. And it is more efficient than Li's solution and has been used to solve the problem of general geometric intersection problem [25]. Luo et al. [22] also present a point-inclusion protocol based on the protocol for the problem of secure computation

of the distance between two private points, but some drawbacks also remain. The BGN homomorphic scheme can allow one multiplication and multiple additive operations over the encrypted data and can be used to solve some SMC problems, but its performance is still slow over composite-order group [3, 8]. Bilogrevic et al. [5] addressed the privacy-preserving problem in Location-Sharing-Based Service based on the BGN and both the Paillier and ElGamal cryptosystem respectively, and they claimed that the Paillier-based solution would have a better performance than BGN-based one. In 2010, Freeman [13] proposed a conversion solution to improve performance of BGN cryptosystem. In the BGN cryptosystem, the plaintext must be restricted to be in some small range(integers less than some bound  $L$ , say  $L = 10^8$ ) and its decryption can be quickly computed in  $O(\sqrt{L})$  time by using Pollard’s kangaroo algorithm, otherwise the discrete logarithm can be very slowly computed, as is a serious disadvantage in some cases. Huang et al. introduced two SMC protocols to compute the distance between two parties’ private vectors, while the first protocol must have a semi-honest third party and the second one was based on randomization technique rather than encryption [15]. Then Huang et al. continued to propose a secure computation protocol for the distance between two private vectors based on privacy homomorphism and scalar product [14], but the performance is not efficient enough for 2-dimensional vector. In 2018, Peng et al. put forward to a quantum protocol to calculate the distance between two private points based on QKD-based effective quantum private query [24]. However, this solution needs  $O(n)$  space complexity and  $O(N \log(N))$  communication complexity, and the fact performance has not been evaluated.

In this paper, we utilize a novel idea based on the Paillier cryptosystem and it can deal with negative value and be used to efficiently solve some secure two-party computational problems in the field of geometry.

### 3 Method of Homomorphic Subtraction of the Paillier Cryptosystem

The Paillier cryptosystem is a probabilistic asymmetric algorithm for public key cryptography [23]. The Paillier cryptosystem is a homomorphic cryptosystem that only supports additive homomorphisms. Even given only the public key and the ciphertext of  $m_1$  and  $m_2$ , we can still calculate  $E(m_1 + m_2) = E(m_1) \cdot E(m_2)$  [21].

**Theorem 1.** *Let  $((n, g), (\lambda, \mu), E, D, Z_n)$  be a Paillier encryption scheme [20],  $f = m_1 \cdot m_2 + m_3 \cdot m_4 + \dots + m_{2i+1} \cdot m_{2i+2} + \dots + m_{2k+1} \cdot m_{2k+2}$ , where  $|m_j| \in Z_n$ ,  $0 \leq i \leq k$ ,  $f \in Z_n$ , we define that  $m'_j = n + m_j$  if  $m_j < 0$  otherwise  $m'_j = m_j$  and  $f' = m'_1 \cdot m'_2 + m'_3 \cdot m'_4 + \dots + m'_{2i+1} \cdot m'_{2i+2} + \dots + m'_{2k+1} \cdot m'_{2k+2}$ , then  $D(E(f)) = D(E(f'))$ .*

*Proof.* Obviously,

$$\begin{aligned} f' &= m'_1 \cdot m'_2 + m'_3 \cdot m'_4 + \dots + m'_{2i+1} \cdot m'_{2i+2} + \dots + m'_{2k+1} \cdot m'_{2k+2}, \\ f &= m_1 \cdot m_2 + m_3 \cdot m_4 + \dots + m_{2i+1} \cdot m_{2i+2} + \dots + m_{2k+1} \cdot m_{2k+2}, \end{aligned}$$

so  $f \equiv f' \pmod n$ ,  $f' = f + k \cdot n$ .

By binomial theorem,

$$(1+n)^x = \sum_0^x \binom{x}{k} \cdot n^k = 1 + n \cdot x + \binom{x}{2} \cdot n^2 + \text{higher power of } n,$$

This indicates that:

$$(1+n)^x \equiv 1+n \cdot x \pmod{n^2}.$$

Generally, let  $g = n + 1$ , therefore,

$$g^{k \cdot n} \pmod{n^2} = (1+n)^{k \cdot n} \pmod{n^2} = (1+k \cdot n \cdot n) \pmod{n^2} = 1.$$

$$\begin{aligned} E(f') &= g^{f'} \cdot r_1^n \pmod{n^2} \\ &= g^{f+k \cdot n} \cdot r_1^n \pmod{n^2} \\ &= g^f g^{k \cdot n} \cdot r_1^n \pmod{n^2} \\ &= g^f \cdot r_1^n \pmod{n^2} \end{aligned}$$

$$E(f) = g^f \cdot r_2^n \pmod{n^2}$$

Thus,

$$D(E(f)) = D(E(f')).$$

### 4 Building Block

An SMC problem for the distance between two private points will be introduced and its protocol will be able to be used as a building block of some other SMC problems in the field of computational geometry. And Protocol 1 will also help to solve other problems in the field of computational geometry.

$$\begin{aligned} |PQ|^2 &= T + D_A(t) \\ &= T + U + 2x_2 \cdot W + 2y_2 \cdot V \\ &= x_1^2 + y_1^2 + x_2^2 + y_2^2 + 2x_2(n - x_1) + 2y_2(n - y_1) \\ &= (x_1 - x_2)^2 + (y_1 - y_2)^2 \end{aligned} \tag{1}$$

Thus, Protocol 1 is correct.

Privacy. In Protocol 1, Alice knows  $x_1, y_1$  and  $|PQ|$ , but she cannot infer  $Q(x_2, y_2)$  from these information. Similarly, Bob only knows  $|PQ|$  and cannot infer  $P(x_1, y_1)$ .

But we notice that Protocol 1 is correct if  $(x_1 - x_2)^2 + (y_1 - y_2)^2 \in \mathbb{Z}_n$ . Let one of the public encryption key parameters of a Paillier cryptosystem be  $n$ , Protocol 1 should be correct if  $0 \leq x_1, y_1, x_2, y_2 < \sqrt{\frac{n}{2}}$  to any two points  $P(x_1, y_1)$  and  $Q(x_2, y_2)$ .

**Protocol 1:** Distance between two private points

**Inputs:** Alice’s private point  $P(x_1, y_1)$  and Bob’s private point  $Q(x_2, y_2)$ .

**Output:** The distance  $|PQ|$  between  $P(x_1, y_1)$  and  $Q(x_2, y_2)$ .

*The protocol:*

1. Setup:
  - Alice generates a key pair for a Paillier cryptosystem and sends the public key to Bob. The corresponding encryption and decryption is denoted as  $E_A(\cdot)$  and  $D_A(\cdot)$ .
2. Alice:
  - (a) computes  $T = x_1^2 + y_1^2, W = n - x_1$  and  $V = n - y_1$ .
  - (b) computes  $E_A(W), E_A(V)$  and sends them to Bob.
3. Bob:
  - (a) computes  $U = x_2^2 + y_2^2$ .
  - (b) computes  $t = E_A(U) \cdot E_A(W)^{2x_2} \cdot E_A(V)^{2y_2}$  and sends it to Alice.
4. Alice:
  - (a) computes  $|PQ| = (T + D_A(t))^{\frac{1}{2}}$ .
  - (b) tells the distance  $|PQ|$  to Bob.

The SMC problem of distance between two private points have been studied [17]. The solution as a building block has been employed in some solutions to solve secure computational problems in the field of geometry. The existing secure two-party computation solution to the problem is based on  $OT_m^1$  oblivious transfer protocol where  $m$  is a security parameter such that  $\frac{1}{m}$  should be small enough. This solution needs 4 times  $OT_m^1$  oblivious transfer, so it is highly inefficient. In general, modular multiplication(or exponentiation) operations are the most time-consuming computation, so modular multiplications will be only counted as the cost. In Protocol 1, our solution only takes 3 times public key encryptions and 1 time decryption which needs about  $7 \log(n)$  times modular multiplications and Li’s solution needs about  $4 \cdot (2m + 3) \log(q)$  times modular multiplications, where  $q$  is a large modulo prime. So our solution is more efficient.

## 5 Relationship Between a Private Circle Area and a Private Point

Li et al. have also studied and solved some other SMC problems in the field of geometry based on the relationship between two private points [22]. We can also apply our Protocol 1 as a new building block to these secure computational geometric problems and these new solutions should be more efficient. In order to illustrate the practical applications of Theorem 1, we also will introduce a more efficient and private solution to secure multi-party computation problem of the relationship between a circle area and a private point.

The solution proposed by Li et al. can determine the relationship between a private circle area and a private point is based on whether the distance between the private point and the center of the private circle is greater than the radius of the circle [17, 22]. For example, Bob decides to bomb a circle area whose center is  $Q(x_2, y_2)$  and radius is  $r$  in another country, Alice has an interesting point of  $P(x_1, y_1)$ . Using Protocol 2 in [17], if Alice knows  $|PQ| > r$  and Bob can bomb the circle area, but if  $|PQ| \leq r$ , Alice can tell her interesting point and Bob cannot bomb the point. If the point  $P(x_1, y_1)$  is not within the circle area, no information should be known by Alice and Bob. Li et al. claims that Protocol 2 in [17] is private, but we find two drawbacks. We describe them as follows.

1. After Protocol 2 in [17] is completed, though Alice cannot know  $Q(x_2, y_2)$  and  $r$ , but she can know that the center point  $Q(x_2, y_2)$  of the circle is on the circumference of a circle whose center is  $P(x_1, y_1)$  and radius is  $|PQ|$ . Figure 1 shows the knowledge known by Alice.

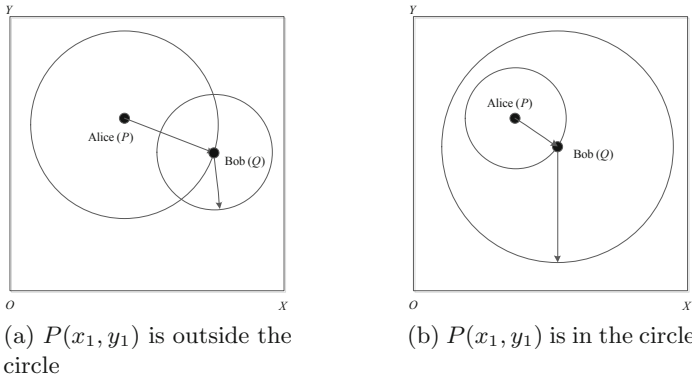


Fig. 1. The knowledge known by Alice after executing Protocol 2 in Li’s solution.

2. Suppose that Alice has more than one point of interest, for example two points,  $P_0(x_0, y_0)$  and  $P_1(x_1, y_1)$ . Alice can compute the possible center point  $Q(x_2, y_2)$  of the circle area according to the following formulas:

$$\begin{cases} |P_0Q| = \sqrt{(x_0 - x_2)^2 + (y_0 - y_2)^2} \\ |P_1Q| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \end{cases} \quad (2)$$

In Ref. [22], Luo et al. also proposed a point-inclusion protocol (Protocol 2) based on their protocol to the secure two-party computation problem of distance between two private points, but some drawbacks still remain. In Protocol 2 [22],

$$\begin{aligned} u' &= (x_0 - a)^2 + (y_0 - b)^2 + v' \\ u'' &= v - v' - r^2 \\ u &= u' + u'' \\ u \stackrel{?}{\leftrightarrow} v &\Leftrightarrow (x_0 - a)^2 + (y_0 - b)^2 \stackrel{?}{\leftrightarrow} r^2 \end{aligned}$$

Suppose that,

$$\begin{cases} (x_0 - a)^2 + (y_0 - b)^2 = n - 5 \\ v' = 8 \\ r^2 = 1 \\ v = 20 \end{cases}$$

$$\begin{aligned} u' &= (x_0 - a)^2 + (y_0 - b)^2 + v' \\ &= n - 5 + 8 \\ &= n + 3 \\ &\equiv 3 \pmod n \\ u &= u' + u'' \\ &= 3 + v - v' - r^2 \\ &= 3 + 20 - 8 - 1 \\ &= 14 \\ u &< v \end{aligned}$$

But, because of the large prime  $n$ ,  $(n - 5) > 1$ , i.e.,  $(x_0 - a)^2 + (y_0 - b)^2 > r^2$ , as is inconsistent with  $u < v$ .

We introduce a new protocol based on our Protocol 1 to the secure multi-party computation of the relationship between a private point and a circle area. Our protocol can get rid of the above-mentioned drawbacks.

Similarly, we notice that Protocol 2 is correct if  $(x_1 - x_2)^2 + (y_1 - y_2)^2 + R \in \mathbb{Z}_n$ . Protocol 2 must be correct if  $0 \leq x_1, y_1, x_2, y_2 < \sqrt{\frac{n}{4}}$  and  $0 \leq r < \sqrt{\frac{n}{2}}$  and  $0 \leq R < \frac{n}{2}$ .

Privacy.

1. Compared with Protocol 2 in Ref. [17], after Protocol 2 is completed, Alice cannot know that the center point  $Q(x_2, y_2)$  of the circle is on the circumference of a circle whose center is  $P(x_1, y_1)$  and radius is  $|PQ|$  due to the random number  $R$ .
2. Even if Alice has more than one point of interest, for example two points,  $P_0(x_0, y_0)$  and  $P_1(x_1, y_1)$ , Alice cannot compute the possible center point  $Q(x_2, y_2)$  of the circle area according to the following formulas due to the random numbers  $R_0$  and  $R_1$ :

$$\begin{cases} u_0=(x_0 - x_2)^2 + (y_0 - y_2)^2 + R_0 \\ u_1=(x_1 - x_2)^2 + (y_1 - y_2)^2 + R_1 \end{cases} \tag{3}$$

So Protocol 2 is more private than Protocol 2 in Ref [17].

**Protocol 2:** Relationship between a private circle area and a private point

**Inputs:** A private point  $P(x_1, y_1)$  and a circle area whose center is  $Q(x_2, y_2)$  and radius is  $r$ .

**Output:** Whether or not  $P(x_1, y_1)$  is outside the circle area.

*The protocol:*

1. Setup:  
Alice generates a key pair for a Paillier cryptosystem and sends the public key to Bob. The corresponding encryption and decryption is denoted as  $E_A(\cdot)$  and  $D_A(\cdot)$ .
2. Alice:
  - (a) computes  $T = x_1^2 + y_1^2$ ,  $W = n - x_1$  and  $V = n - y_1$ .
  - (b) computes  $E_A(W)$ ,  $E_A(V)$  and sends them to Bob.
3. Bob:
  - (a) computes  $U = x_2^2 + y_2^2$  and generates a random number  $R$ .
  - (b) computes  $t = E_A(U + R) \cdot E_A(W)^{2x_2} \cdot E_A(V)^{2y_2}$  and sends it to Alice.
  - (c) computes  $v = r^2 + R$ .
4. Alice computes  $u=T + D_A(t)$  and Alice and Bob can decide which of  $u$  and  $v$  is larger by using Yao’s Millionaire protocol. If  $u > v$ , then  $P(x_1, y_1)$  is outside the circle area; and if  $u \leq v$ , then  $P(x_1, y_1)$  is in the circle area, or on the circumference.

## 6 Efficiency Analysis and Experiment Results

In this paper, we introduce a secure two-party computation protocol to distance between two private points based on the Paillier cryptosystem supporting subtraction. Li’s solution is based on  $OT_m^1$  Oblivious Transfer protocol, where  $m$  is



a security parameter such that  $\frac{1}{m}$  is small enough. Their solution needs 4 times  $OT_m^1$  oblivious transfer. As we mentioned before, modular exponentiation operation is the most time-consuming computation.  $OT_m^1$  Oblivious Transfer protocol takes  $2m + 3$  times modular exponentiations, and one Paillier cryptosystem encryption takes modular exponentiation only once and one decryption also takes modular exponentiation only once [21]. Based on the above discussion, we summarize the results of time-consuming in Table 1 and communication cost in Table 2. Results show that the computational cost of our solution is the same as Luo's, and the communication traffic is less than Luo's. And both of Luo's and our solutions are more efficient than Li's solution.

**Table 1.** Comparison of computational time-consuming results.

Protocol	Alice	Bob	Total
Li's solution [17]	12	$8m$	$8m + 12$
Luo's solution [22]	2	3	5
Ours (Protocol 1)	2	3	5

Note: computation cost is measured in the number of modular exponentiations.

**Table 2.** Comparison of communication cost results.

Protocol	Communication traffic	Rounds
Li's solution [17]	$8m + 4$	$9^a$
Luo's solution [22]	4	3
Ours (Protocol 1)	3	$3^a$

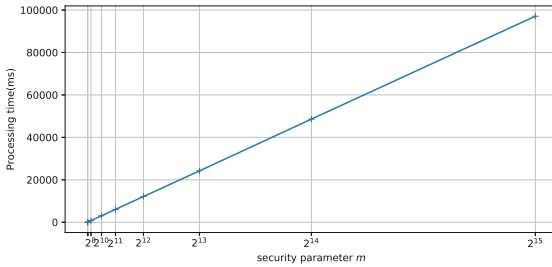
Note: communication cost is measured in the number of large numbers and the number of communication rounds.

<sup>a</sup>The last round in Li's solution and our solution is not in Luo's solution, so it is not counted while comparing.

To better compare the actual computational cost of our solution based on the Paillier homomorphic cryptosystem supporting subtraction and Li's solution based on  $OT_m^1$  Oblivious Transfer protocol, we implement our Protocol 1 and Li's solution [17] based on Charm-Crypto framework in Python 2.7. We build the Charm-Crypto framework based on GMP 6.0.0 without the side-channel silent `mpz_powm_sec` function. All experiments were performed on a computer running the Ubuntu subsystem on a Windows 10 system with a 3.50 GHz Intel i5-4690 processor and 8 GB of RAM. The results are summarized in Table 3 and Fig. 2.

**Table 3.** Experiment results of Li’s solution.

Security parameter $m$	Processing time (ms)
$2^1$	9
$2^5$	98
$2^8$	760
$2^{10}$	3037
$2^{11}$	6053
$2^{12}$	12113
$2^{13}$	24233
$2^{14}$	48609
$2^{15}$	97096



**Fig. 2.** Processing time vs. security parameter  $m$ .

From Table 3 and Fig. 2, we can see that as security parameter  $m$  increases linearly the cost of Li’s solution is increased linearly. If Bob chooses to guess, his chance of guessing the correct  $x_1$  is  $\frac{1}{m^2}$ . So the chance that Bob guesses the correct point  $P(x_1, y_1)$  is  $\frac{1}{m^4}$ , which should be small enough. Li’s solution should be secure while the probability of a random guess is  $\frac{1}{2^{80}}$ , and the processing time is about 52 min. Except for the key setup and the decrypting time, the processing time of our Protocol 1 is only 4 ms and the total processing time is about 8 ms while the key length of  $n$  is 1024 bits (80-bit AES security level) and encryption operation can be simplified to  $(nm + 1) \cdot r^n \pmod{n^2}$ . In summary, our Protocol 1 is more effective and practical based on the Paillier cryptosystem than Li’s one based on  $OT_m^1$  Oblivious Transfer protocol.

In addition, we also compare the fact computation cost of our solution based on the Paillier cryptosystem and the solution based on the BGN cryptosystem. The BGN cryptosystem is also implemented using Python 2.7 based on Charm-Crypto. The reasonable solution can also be easily constructed based on the BGN cryptosystem by multiplication in ciphertext space and omitted in this paper. The discrete logarithm is computed by using Pollard’s kangaroo algorithm. In Table 4, the BGN cryptosystem is tested based on composite-order group (Type

a1 pairing, Base field size is 1024 bits) and primer-order group (Type f pairing, Base field size is 160 bits) at 80-bit security level, respectively [4, 8].

**Table 4.** Processing time (ms) of two solutions based on BGN ( $L = 10^8$ ) and Paillier at 80-bit security level.

Protocol phase	BGN (composite-order)	BGN (prime-order)	Paillier
Setup	56.6	152.5	2.7
Protocol execution	130.4	140.1	4
Result decryption	430.5	7442	1.3

Overall, Table 4 shows that our solution is also more efficient based on the Paillier cryptosystem than the solutions base on the BGN cryptosystem over composite-order and prime-order group at 80-bit security level. In addition, the plaintext of the BGN-based solution must be restricted to be in some small range  $L$ , and its decryption can be quickly computed in  $O(\sqrt{L})$  time. It is a serious disadvantage if the plaintext needs to be in some large range. The plaintext of our solution can be in some large range  $L$  (for example  $L = 2^{1024}$  and  $0 \leq x, y < 2^{511}$  at 80-bit security level in Protocol 2. However, the plaintext of the BGN-based solution must be restricted to be in some small range  $L$ , for example  $L = 10^8$  and  $0 \leq x, y < 5000$ . So our solution based on Paillier cryptosystem is better while the plaintext can be in some large range.

## 7 Conclusion and Future Work

We have introduced a method and application of homomorphic subtraction in the Paillier cryptosystem. It is a novel idea and very useful in the fields of secure multi-party computational geometry. We have used it to solve the secure two-party computation problem for the distance between two private points, which can also be used as a building block of some other secure multi-party computational problems in the field of geometry. Our solution is more efficient and private than Li's solution. Moreover, our protocol is also more efficient than the solution based on the BGN scheme. The plaintext of our solution can be in some large range, but the BGN scheme must be restricted to be in some small range. So our solution based on Paillier cryptosystem is better while the plaintext can be in some large range. We also have addressed some drawbacks in Li's and Luo's solution. There are some interesting secure multi-party computational problems in the field of geometry that can be studied based on our idea. For example, we will study the secure multi-party computational problem for the relationship between a private point and a private polygon area and propose some efficient solutions to them. Moreover, we also think that our method can be used in some other security fields.

## References

1. Agrawal, R., Srikant, R.: Privacy-preserving data mining. In: Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, SIGMOD 2000, pp. 439–450. ACM, New York (2000)
2. Atallah, M.J., Du, W.: Secure multi-party computational geometry. In: Dehne, F., Sack, J.-R., Tamassia, R. (eds.) WADS 2001. LNCS, vol. 2125, pp. 165–179. Springer, Heidelberg (2001). [https://doi.org/10.1007/3-540-44634-6\\_16](https://doi.org/10.1007/3-540-44634-6_16)
3. Au, M.H., Liu, J.K., Fang, J., Jiang, Z.L., Susilo, W., Zhou, J.: A new payment system for enhancing location privacy of electric vehicles. *IEEE Trans. Veh. Technol.* **63**(1), 3–18 (2014)
4. Barker, E., Barker, W., Burr, W., Polk, W., Smid, M.: NIST SP800-57: recommendation for key management part 1: general (revised). Technical report, NIST (2007)
5. Bilogrevic, I., Jadliwala, M., Joneja, V., Kalkan, K., Hubaux, J.P., Aad, I.: Privacy-preserving optimal meeting location determination on mobile devices. *IEEE Trans. Inf. Forensics Secur.* **9**(7), 1141–1156 (2014)
6. Yang, B., Yang, C.H., Yu, Y., Xie, D.: A secure scalar product protocol and its applications to computational geometry. *J. Comput.* **8**(8), 2018–2026 (2013)
7. Bogetoft, P., et al.: Secure multiparty computation goes live. In: Dingledine, R., Golle, P. (eds.) FC 2009. LNCS, vol. 5628, pp. 325–343. Springer, Heidelberg (2009). [https://doi.org/10.1007/978-3-642-03549-4\\_20](https://doi.org/10.1007/978-3-642-03549-4_20)
8. Boneh, D., Goh, E.-J., Nissim, K.: Evaluating 2-DNF formulas on ciphertexts. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 325–341. Springer, Heidelberg (2005). [https://doi.org/10.1007/978-3-540-30576-7\\_18](https://doi.org/10.1007/978-3-540-30576-7_18)
9. Dachman-Soled, D., Malkin, T., Raykova, M., Yung, M.: Efficient robust private set intersection. *Int. J. Appl. Cryptol.* **2**(4), 289–303 (2012)
10. Du, W., Atallah, M.J.: Privacy-preserving cooperative scientific computations. In: Proceedings of the 14th IEEE Workshop on Computer Security Foundations, CSFW 2001, Washington, DC, USA, pp. 273–282. IEEE Computer Society (2001)
11. Du, W., Han, Y.S., Chen, S.: Privacy-preserving multivariate statistical analysis: linear regression and classification. In: Proceedings of the 4th SIAM International Conference on Data Mining, Lake Buena Vista, Florida, vol. 233, pp. 222–233 (2004)
12. Freedman, M.J., Nissim, K., Pinkas, B.: Efficient private matching and set intersection. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 1–19. Springer, Heidelberg (2004). [https://doi.org/10.1007/978-3-540-24676-3\\_1](https://doi.org/10.1007/978-3-540-24676-3_1)
13. Freeman, D.M.: Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 44–61. Springer, Heidelberg (2010). [https://doi.org/10.1007/978-3-642-13190-5\\_3](https://doi.org/10.1007/978-3-642-13190-5_3)
14. Huang, H., Gong, T., Chen, P., Malekian, R., Chen, T.: Secure two-party distance computation protocol based on privacy homomorphism and scalar product in wireless sensor networks. *Tsinghua Sci. Technol.* **21**(4), 385–396 (2016)
15. Huang, H., Gong, T., Chen, P., Qiu, G., Wang, R.: Secure two-party distance computation protocols with a semihonest third party and randomization for privacy protection in wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **11**(7), 475150 (2015)

16. Jha, S., Kruger, L., McDaniel, P.: Privacy preserving clustering. In: di Vimercati, S.C., Syverson, P., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 397–417. Springer, Heidelberg (2005). [https://doi.org/10.1007/11555827\\_23](https://doi.org/10.1007/11555827_23)
17. Li, S.D., Dai, Y.Q.: Secure two-party computational geometry. *J. Comput. Sci. Technol.* **20**(2), 258–263 (2005)
18. Lindell, Y., Pinkas, B.: Privacy preserving data mining. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 36–54. Springer, Heidelberg (2000). [https://doi.org/10.1007/3-540-44598-6\\_3](https://doi.org/10.1007/3-540-44598-6_3)
19. Liu, L., Wu, C., Li, S.: Two privacy-preserving protocols for point-curve relation. *J. Electron. (China)* **29**(5), 422–430 (2012)
20. Liu, M., et al.: Privacy-preserving matrix product based static mutual exclusive roles constraints violation detection in interoperable role-based access control. *Future Gener. Comput. Syst.* (2018)
21. Liu, M., Zhang, X., Yang, C., Pang, S., Puthal, D., Ren, K.: Privacy-preserving detection of statically mutually exclusive roles constraints violation in interoperable role-based access control. In: 2017 IEEE Trustcom/BigDataSE/ICCESS, pp. 502–509. IEEE (2017)
22. Luo, Y.L., Huang, L.S., Zhong, H.: Secure two-party point-circle inclusion problem. *J. Comput. Sci. Technol.* **22**(1), 88–91 (2007)
23. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999). [https://doi.org/10.1007/3-540-48910-X\\_16](https://doi.org/10.1007/3-540-48910-X_16)
24. Peng, Z., Shi, R., Wang, P., Zhang, S.: A novel quantum solution to secure two-party distance computation. *Quantum Inf. Process.* **17**(6), 1–12 (2018). <https://doi.org/10.1007/s11128-018-1911-0>
25. Qin, J., Duan, H., Zhao, H., Hu, J.: A new lagrange solution to the privacy-preserving general geometric intersection problem. *J. Netw. Comput. Appl.* **46**, 94–99 (2014)
26. Shih, D.H., Huang, H.Y., Yen, D.C.: A secure reverse Vickrey auction scheme with bid privacy. *Inf. Sci.* **176**(5), 550–564 (2006)
27. Xie, Q., Hengartner, U.: Privacy-preserving matchmaking for mobile social networking secure against malicious users. In: Proceedings of the 2011 Ninth Annual International Conference on Privacy, Security and Trust (PST), pp. 252–259. IEEE (2011)
28. Xiong, H., Zhang, E., Chim, T., Yiu, S., Hui, L.C.K.: Weighted average problem revisited under hybrid and malicious model. In: Proceedings of the 2012 8th International Conference on Computing Technology and Information Management, vol. 2, pp. 677–682 (2012)
29. Yang, B., Shao, Z., Zhang, W.: Secure two-party protocols on planar convex hulls. *J. Inf. Comput. Sci.* **9**(4), 915–929 (2012)
30. Yang, B., Sun, A., Zhang, W.: Secure two-party protocols on planar circles. *J. Inf.* **8**(1), 29–40 (2011)
31. Yao, A.C.: Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, SFCS 1982, Washington, DC, USA, pp. 160–164. IEEE Computer Society (1982)