Key Technologies and Applications of Secure Multiparty Computation

Xiaoqiang Guo*, Shuai Zhang, Ying Li
College of Science, Hebei United University,
No.46 Xinhua West Street, Tangshan, 063009, Hebei Province, China
Corresponding author, e-mail: guoxiaoqiang@heuu.edu.cn, guoxq2004@163.com

Abstract

With the advent of the information age, the network security is particularly important. The secure multiparty computation is a very important branch of cryptography. It is a hotspot in the field of information security. It expanded the scope of the traditional distributed computing and information security, provided a new computing model for the network collaborative computing. First we introduced several key technologies of secure multiparty computation: secret sharing and verifiable secret sharing, homomorphic public key cryptosystem, mix network, zero knowledge proof, oblivious transfer, millionaire protocol. Second we discussed the applications of secure multiparty computation in electronic voting, electronic auctions, threshold signature, database queries, data mining, mechanical engineering and other fields.

***Keyword**: secure multiparty computation, secret sharing, zero knowledge proof, electronic auctions, threshold signature*

1. Introduction

With the rapid development of computer networks, mankind has entered the information society. Use of the internet to obtain information, exchange information and work together has become a very important feature of the information society. Information technology to bring people the material and cultural enjoyment, at the same time information security issues have become increasingly prominent. Network intrusion, information leaks and cybercrime and other cases are also rising. Therefore, how to block the network security vulnerabilities and eliminate security risks has become a great concern and attention problems.

Secure multiparty comutation is an important research direction in the field of information security. It expanded the scope of the traditional distributed computing and information security, provided a new computing model for the network collaborative computing. It is of an important value to solve the information security in the network environment.

In 1982, A.C. Yao proposed the two-party secure computation through Yao's millionaires problem [1]. O. Goldreich, S. Micali and A. Wigderson presented secure multiparty comutation that can be calculated any function based on the cryptography security agreement [2]. They prove that there exist n-secure protocol when the presence of passive attacks and $n-1$-secure protocol when the presence of active attacks. D. Chaum, C. Crepeau and I. Damgard studied on secure multiparty comutation in information theory security model [3]. They prove that there exist $n-1$-secure protocol under passive attacks and $\left\lfloor \frac{n}{2} \right\rfloor - 1$-secure protocol under active attacks. S. Goldwasser and L. Levin researched secure multiparty comutation in the case of that computing model has been bribed by the majority of agreement participants [4]. O. Goldreich, S. Goldwasser and N. Linial studied on secure multiparty comutation protocols in the case of that insecure communication channel, the attacher with unlimited computing power [5]. R. Ostrovsky and M.Yung studied on the mobile adversaries under secure channel model [6]. S. Micali, P. Rogaway and Beaver gave the formal definition of secure multiparty comutation under secure channel model [7,8].

In this paper, we mainly introduce several key technologies of secure multiparty computation: secret sharing and verifiable secret sharing, homomorphic public-key

Received January 27, 2013; Revised April 16, 2013; Accepted April 28, 2013

cryptosystem, mix network, zero-knowledge proof, oblivious transfer, millionaire protocol in section 2. And we discuss the application of secure multiparty computation in electronic voting, electronic auctions, threshold signature, database queries, data mining, mechanical engineering and other fields in section 3.

2. Key Technologies of Secure Multiparty Computation

2.1. Secret Sharing and Verifiable Secret Sharing

Secret sharing is a distributed, save and restore the secret method. It is an important tool for achieving secure multiparty computation. Threshold secret sharing (t,n) is the most common secret sharing system. Secret $s=\{s_1,s_2,\cdots,s_n\}$ deposited with n members $\{P_1,P_2,\cdots,P_n\}$, need at least t members to reconstruct s. Even $t-1$ members together, any information about s cannot be obtained. When t or more information is available on uniquely and efficiently reconstruct s. In the early programs assume that all parties involved are honest, that is Bob and secret sharer $P_i(1\le i\le n)$ provided the secret corret, therefore not be able to resist malicious attacker cheating. For this reason, in the secret distribution process, increase the authentication protocol to ensure each of $P_i(1\le i\le n)$ can be verify the correctness Bob distributing secret, and achieve verifiable secret sharing. If any member in the system (including external members) can verify the correctness of the secret s_i, called publicly verifiable secret sharing. For n participants, in [9], the program based on Double Discrete Logarithms assumption, and its complexity is $O(k^2n)$, where k is at least 1024 bits to reach security. In [10], the program based on Diffie-Hellman assumption, in any group of calculating the discrete logarithm infeasible, its complexity reduced $O(kn)$.

2.2. Homomorphic Public Key Cryptography

Assume S is a public key cryptography, k is its security parameter, X represents a message space, C represents a ciphertext space, and X is an Abel additive group, C is an Abel multiplicative group, $\{0,1\}^k$ represents a random bit string of the length k, E_k represents public encryption function, D_k represents public decryption function. $\forall x_1,x_2\in X$, $u_1,u_2\in\{0,1\}^k$, if $E_k(u_1,x_1)$ and $E_k(u_2,x_2)$ are calculated indistinguishable, then S is called semantically secure, or S is cryptography security. Further, if there exists $u\in\{0,1\}^k$ to make $E_k(u,x_1+x_2)=E_k(u_1,x_1)\cdot E_k(u_2,x_2)$, then S is called semantically secure homomorphic public key cryptography.

S. Goldwasser and S. Micali put forward the first probabilistic pubic key encryption scheme [11], called Goldwasser-Micali (GM) scheme. GM scheme is additively homomorphic. Its security is based on Quadratic Residue assumption. ρ is the message extension rate of the encryption algorithm, and $\rho=\log_2 N$, where security parameter $N=pq$. The bit complexity of the cryptographic operation on the message m is $O(|m|(\log_2 N)^2)$, so GM encryption system is inefficient.

T. ElGamal proposed homomorphic probabilistic cryptosystem [12]. It is multiplicaivaly homomorphic to realize secure multiparty multiplication of the encrypted data. Its security is based on Decision Diffie-Hellman assumption. Its shortcoming is that message expansion rate of the encryption scheme on the finite field is tremendous, to achieve practical security, large prime number p needs at least 300 decimal digits, its bits length $|p|$ at least 1024, and at least there should be a large prime factor of $p-1$.

J. Benaloh proposed homomorphic dense probabilistic encryption scheme [13]. It is extension of the GM program, similar to the GM program, also additively homomorphic. Its security is based on the High-degree Residuosity problem, message expansion rate ρ close to 1.

P. Paillier proposed homomorphic probabilistic public key encryption algorithm [14], which is additively homomorphic. Its security is based on the Decisional Composite Residuosity assumption, message expansion rate ρ is a constant.

2.3. Mixnets Protocol

Mixnets is basic cryptographic protocols of anonymously send, which concept was firstly proposed by D. Chaum in [15]. The Mixnets is consitituted by a collection of servers, the original information input mixnets, through multiple secret permutation, then output. The process hide the relationship between the output message and the sender and achieve anonymous sending a message.

Protocol 1. Mixnets Protocol

System parameters: suppose n mixnets servers $S_1, S_2, \cdots, S_n$, each S_i generate a pair of keys (P_{K_i}, S_{K_i}), S_i open the pubic key P_{K_i} and keep secret own private key S_{K_i}.

Input stage: each sender perform the following encryption to the sending message m:

$$E_{P_{K_1}}(E_{P_{K_2}}(\cdots E_{P_{K_n}}(m)))$$

then send to S_1.

Mixed stage:

Step 1. When enough members send their own message to S_1, S_1 use his own private key S_{K_1} to decrypt all received messages. S_1 randomly permute all the messages and send $E_{P_{K_2}}(\cdots E_{P_{K_n}}(m))$ to S_2.

Step 2. S_2 use private key S_{K_2} to decrypt all received messages, and randomly permute all. S_2 send $E_{P_{K_3}}(\cdots E_{P_{K_n}}(m))$ to S_3.

Step 3. For $S_3, \cdots, S_n$, perform the above same operation.

Output stage: S_n output original sequence.

Because the output ciphertext is randomly permutation of input, the attacker cannot determine the correspondence between of them. The length of encrypted message and the amount of user computing are proportional to the number of mixnets servers. When many users, the efficiency is very low.

2.4. Zero Knowledge Proof

Zero knowledge proof is a basic method of cryptography, the purpose is prover P manage to make verifier Q believe in himself master some secret information, but at the same time not leak these secret information to Q. According to whether between prover and verifier need interaction, zero knowledge proof protocol divided into interactive and non-interactive. According to the different of system security and attacker model in the zero knowledge proof process, we need to further study complete zero knowledge, statistical zero knowledge, calculation zero knowledge, honest verifier zero knowledge and so on protocols, to adapt to the different areas of secure multiparty comutation.

2.5. Oblivious Transfer

Oblivious transfer is agreement in order to secretly achieve the part message from a collection of messages. In 1981, M. Rabin first proposed the concept of oblivious transfer and gave 1-out of-2 OT_2^1 protocol based on factorization problem [16]. A.C. Yao constructed the first oblivious circuit valuation agreement based on OT_2^1 protocol. L. Hard and H. Lin gave a OT_2^1 protocol based on Discrete Logarithm problem. Then OT_n^1 and OT_n^m have been successively proposed.

Protocol 2. OT_2^1 protocol

Target: Alice sent a secret to Bob, Bob got the secret with probability of $\frac{1}{2}$.

System parameters: Alice chose two secret large prime numbers $p,q, p \times q = N$, p,q keeping secret, N open.

Procedure:

Step 1. Alice sent N to Bob.

Step 2. Bob randomly chose $x \in [1, N-1]$ and sent $x^2 \equiv a \pmod N$ to Alice.

Step 3. Alice used the value of p,q and the Chinese Residuosity Theorem to calculate secondary roots $x, N-x, y, N-y$, and sent any one to Bob.

Step 4. If Bob received y , then he can calculate $\gcd(x+y, N) = p$. If he received $N-y$, then he can calculate q . If not, Bob cannot get the Alice's secret p,q .

2.6. Millionaire Protocol

Millionaire protocol is also called secret comparison protocol, which aim is to compare two secret data size. It was proposed by Turing Award winner A.C. Yao. The purpose is to compare which is richer two millionaires in the case not to expose their wealth. Therefore the problem is also known as Yao's millionaires problem [1].

Protocol 3. Yao's millionaire protocol

Input: Alice put in secret number i , Bob put in secret number j .

Output: Alice and Bob safely calculated function $GT = (i, j) = [i > j]$. If $GT = (i, j) = 1$, then $i > j$ set up. If not, $GT = (i, j) = 0$, $i \leq j$.

The communication complexity of Yao's early program is exponentially. Comparing the two numbers of the bit length l , consideration is $\theta(2^l)$, only suitable for two little secret data comparing. In order to improve the protocol efficiency, C. Cachin introduced an untrusted third party and proposed an higher efficient comparison program [17]. The program is based on φ -hiding assumption, comparing the two data of bit length l , the communication complexity is $O(l)$. The untrusted third party is a semi-honest or oblivious, allowing to participate in the protocol, but he cannot get Alice and Bob's private information and the final results, and also cannot collude with any participant.

3. Applications of Secure Multiparty Computation

3.1. Electronic Voting

In the society of the future, electronic voting will greatly promote the democratization process and play an important role in ensuring the rights of citizens, protecting citizen's freedom and privacy. Electronic voting protocol is a typical application of secure multiparty computation. It has also been extensive attention of researchers. After the satisfied nature of a secure multiparty computation specific, we can get some properties of electronic voting protocol: the integrity of the voting count, the robustness of the voting process, the confidentiality, irreproducible, verifiability of the ballot.

3.2. Electronic Auction

Electronic auction is a very representative application of secure multiparty computation. It is more and more attention, but users suspected the legitimacy of the online auction because of the problem of security and privacy, especially in the large internet trading areas. Electronic auction is a very active service in the e-commerce. Now many electronic auction scheme has been proposed, most of which are based on verifiable secret sharing. Efficient and secure electronic auction protocol is the focus of current research. Generally, an electronic auction protocol has the nature of confidentiality, irreproducible, verifiability etc.

3.3. Threshold Signature

Threshold signature is the most well-known examples of secure multiparty computation. Its technology is already quite mature. With the widespread launch of e-commerce activities, CA as a trusted institution play an important role increasingly. CA's security ia also an important problem. If a master key of the CA in one place, will also be a safety hazard. Threshold signature can solve this problem and own the following benefits:

1) The master key is not in one place, but to share in a group of servers. Even if some servers are attacked, it do not disclose the master key.

2) Even if some servers are attacked, it is unable to perform the signature tasks. Other services can also continue to maintain the function of CA to complete the signature tasks. The CA's security can be greatly improved [18].

3.4. Database Query

In database query, if you can guarantee that the users only get the query results,but do not understand the database record information, at the same time, the party owned database do not know users which to query a record, the query process is called a safety query. The query problem has broad application prospects in the field of secure multiparty computation. For example, multiple intelligence sector cooperation query. Assume department A want to query database of department B, the query conditions of A is sensitive information and cannot be leaked to B, but B have privacy implications record, B should be as much as possible to ensure data records not to leak for the record A dose not query. The above scenario is typical application for safety query. Security query problem is widespread in various fields of business competition and military cooperation etc.

3.5. Data Mining

With the development of society, people generate and collect data and the amount of information are sharp increasing. Thus sensitive data collection, agencies cooperation, operations of transnational corporations presented new challenges to data mining, privacy and security problems. Privacy mining is an emerging research direction and mainly consider two aspects:

1) Sensitive raw data.
2) The sensitive knowledge extracted from database should be deleted because it is likely to jeopardize the privacy of others.

The main purpose of privacy mining is to use some technology to improve the existing data mining algorithms to modify the original data and make sensitive data and knowledge not disclosed [19].

3.6. Mechanical Engineering Field

With the globalization of market competition, the machinery manufacturing industry is facing more intense global competition in the market. The production mode gradually transformed from a few varieties, large quantities to many varieties, variable volume. The process of design and manufacture of the product developed by a business alone to a strong alliance between the complementary enterprises. Thus, offsite design and manufacture of the product, agile manufacturing technology, virtual manufacturing technology etc. advanced manufacturing mode and technology is becoming hot and key areas of manufacturing engineer researches and applications. However, there is competition, how to cooperate under the premise of protecting their trade secrets? It is very necessary to secure multiparty computation in a distributed design.

In recent years, many scholars have introducted secure multiparty computation technology into the traditional data mining, calculated geometry, private information retrieval, statistical analysis etc.

4. Conclusion

Research on secure multiparty computation is a hotspot in international cryptography. In this paper, we mainly introduced several key technologies and applications of secure multiparty computation. Finding a safe and effective without trusted third party multiparty computation protocols and using formal methods to define and prove the security of party multiparty computation protocols are open. They have a very important significance for elimination hidden of the existing protocol security vulnerabilities.

Acknowledgements

This work was supported by the Scientific Technology Research and Development Plan Project of Tangshan (No. 121302001a).

References

[1] Yao AC. Protocols for Secure Computations. Proc. 23rd IEEE Symp on the Foundation of Computer Science. 1982: 160-164.

[2] Goldreich O, Micali S, Wigderson A. How to Play Any Mental Game. Proc. 19th ACM Symp on the Theory of Computing. 1987: 218-229.

[3] Chaum D, Crepeau C, Damgardl. *Multiparty Unconditionally Secure Protocols (extended abstract)*. Proc. 20th ACM Symp on the Theory of Computing. 1988: 11-19.

[4] Goldwasser S, Levin L. Fair Computation of General Functions in Presence of Immoral Majority. *Advances in Cryptology-CRYPTO of LNCS*. Springer-Verlag. 1990; 537.

[5] Goldreich O, Goldwasser S, Linial N. *Fault-Tolerant Computation in the Full Information Mode1*. Proc. 32nd FOCS. 1991: 447-457.

[6] Ostrovsky R, Yung M. *How to Withstand Mobile Virus Attacks*. Proc. 10th ACM Symp on Principles of Distributed Computing. 1991: 51-59.

[7] Micali S, Rogaway P. Secure Computation. *CRYPTO*. 1991.

[8] Beaver D. Foundations of Secure Interactive Computing. *CRYPTO*. 1991.

[9] Stadler M. Publicly Verifiable Secret Sharing. *Advances in Cryptology-EUROCRYPT 96 LNCS1070*. Berlin: Springer—Verlag. 1996: 190-199.

[10] Schoenmaker B. A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting. *Advances in Cryptology-CRYPTO LNCS1666*. Berlin: Springer-Verlag. 1999: 148-164.

[11] Goldwasser S, Micali S. Probabilistic Encryption. *Journal of Computer and System Sciences*. 1984; 28(2): 270-299.

[12] E1Gamal T. A Public-Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*. 1985; 31(4): 469-472.

[13] Benaloh J. Dense Probabilistic Encryption. Proc. of the Workshop on Selected Areas of Cryptography. Kingston, Canada. 1994: 120-128.

[14] Paillier P. Public-Key Crytosystems Based on Composite Degree Residuosity Classes. *Advances in Cryptology EUROCRYPT LNCS1592*. Berlin: Springer-Verlag. 1999: 223-238.

[15] Chaum D. Untraceable Electronic Mail. Return Addresses and Digital Pseudonyms. *Communications of the ACM*. 1981; 24(2): 84-88.

[16] Rabin M. How to Exchange Secrets by Oblivious Transfer. *Technical Report. Aiken Computation Laboratory*. Harvard University. 1981.

[17] Cachin C. Efficient Private Bidding and Auctions with an Oblivious Third Party. Proc of 6th ACM Conference on Computer and Communications Security. New York: ACM Press. 1999: 120-127.

[18] Wenjun L. Secure Multiparty Computation Theory and Its Applications. PhD Thesis. Gui Yang: Guizhou University. 2005.

[19] Yun C, Wei Z. Study on Privacy Preserving Data Mining Method. *Computer Information*. 2006; 22: 239-241.