ONLINE CONSECUTIVE SECURE MULTI-PARTY COMPUTATION ALGORITHM FOR PRESERVING PRIVACY

ABDOLREZA RASOULI KENARI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

NOVEMBER 2011

O' brother, you are all (in Fact) Thought

The rest, you are the Bones and Meat

Jalal al-Din Rumi

ای برادر تو همه اندیشه‌ای

To my beloved mother and father
to my loving wife
and Ilia

ACKNOWLEDGEMENT

In the name of God, the Most Gracious, the Most Merciful. I would like to express my deep and sincere gratitude to my supervisor, Professor Dr Mohd Aizaini Maarof and in memory of Dr Mohd Nor Mohd Sap (God bless him). Their wide knowledge and their logical way of thinking have been of great value for me. Their understanding, encouraging and personal guidance have provided a good basis for the present thesis.

I also wish to thank Meghdad PhD of English education, for revising the English of my manuscript and Alyda binti Othman from *MalayExpressions* for her proofread and editing services. During this work, I have collaborated with many colleagues for whom I have great regard, and I wish to extend my warmest thanks to all those who have helped me with my work in the Faculty of Computer Science and Information Systems, University of Technology, Malaysia.

I owe my loving thanks to my wife Mahboubeh, my son Illia and our parents. They have lost a lot due to my research abroad. Without their encouragement and understanding, it would have been impossible for me to finish this work. My special gratitude is due to my family, my sister and brothers, their families for their loving support.

ABSTRACT

Every day large volume of information produces and stores among multi parties systems. Although these data are produced by companies unrelated to each other and are stored in various parties, but when they are gathered together much valuable information and patterns reveals. Data mining over distributed data discovers this costly knowledge. However, ownership of data by different companies and maintain confidentiality of data is the main challenge in this research. Secure Multi-party Computation is a set of methods that perform mathematic computation over the multi-party distributed data with ensuring the privacy preserving of the confidential data. Most of these methods use a shared secret key to ensure the privacy of each party. All parties should be present to share the secret keys, but unfortunately, in many applications, the parties are not joining the process at the start time. The aim of this research is to design a new online consecutive secure multi-party computation algorithm. The main problems addressed in this research are the online secret sharing and the consecutively two-party computation. The infinite convergent product sequences are employed to overcome the dependency problem between the shared secret key and users' public keys, which make the algorithm runs offline. The designed online secret sharer allows the parties to join the system during process life. The second problem is cleared by adding a two-party computation randomizer to the system. The two-party randomizer ensures the privacy of the online consecutive computation. The designed algorithm is tested and the result proves the security and applicability of the algorithm. Moreover, a distributed online frequent itemset mining is developed using the proposed algorithm and the result demonstrates the performance, efficiency and practicability of the multi-party computation algorithm. The result shows that the algorithm lasts only 0.5 second for thousand of the parties in offline mode and 27 minutes in the case of online mode with millions of participants.

ABSTRAK

Kebanyakan penghasilan dan penyimpanan maklumat dilaksanakan dalam sistem pelbagai pihak dalam kuantiti yang besar. Walaupun penghasilan data oleh syarikat yang tiada berkaitan antara satu sama lain akan disimpan oleh pelbagai pihak, namun begitu apabila data ini dikumpulkan bersama maka berlaku banyak pendedahan maklumat dan corak data yang berharga. Perlombongan dalam penyebaran data menyebabkan penemuan pengetahuan yang berharga ini. Walaubagaimanapun, pemilikan data oleh pelbagai syarikat yang berbeza dan juga, penyelenggaraan kerahsiaan data tersebut adalah cabaran utama penyelidikan ini. Pengiraan Pelbagai Pihak Yang Terjamin adalah satu set kaedah yang mengaplikasikan pengiraan matematik ke atas penyebaran data-data sulit bagi memastikan pemeliharaan kerahsiaan data tersebut. Kebanyakan kaedah tersebut menggunakan perkongsian kekunci kerahsiaan untuk memastikan pemeliharaan kerahsiaan data bagi setiap pihak. Semua pihak yang terlibat dikehendaki untuk mengemukakan kekunci kerahsiaan untuk dikongsi bersama, namun begitu, kenyataannya mereka tidak menyertai proses pada masa permulaan. Tujuan penyelidikan ini adalah untuk merekabentuk satu algoritma yang baru Pengiraan Pelbagai Pihak Terjamin Berturutan Atas Talian. Masalah utama yang ingin diselesaikan ialah berkenaan perkongsian kerahsiaan atas talian dan pengiraan berturutan antara dua pihak. Perlaksanaan turutan produk pemusatan infiniti ialah untuk menyelesaikan masalah kebergantungan perkongsian kekunci kerahsiaan dan kekunci awam pihak pengguna menyebabkan perlaksanaan algoritma jalankan luar talian. Algoritma yang direkabentuk membolehkan perkongsian kerahsiaan atas talian oleh pelbagai pihak memasuki sistem semasa sesi kitaran proses. Permasalahan kedua yang ingin diselesaikan ialah penambahan pengiraan dua pihak secara rawak ke dalam sistem. Kedua-dua pihak yang dirawakkan membolehkan kerahsiaan ke atas pengiraan berturutan atas talian dilaksanakan. Algoritma yang direka bentuk telah diuji dan keputusan membuktikan keselamatan dan kebolehgunaan algoritma. Selain itu, perlombongan penyebaran set item berfrekuensi atas talian telah dibangunkan menggunakan cadangan algoritma tersebut dan keputusan menunjukkan prestasi, kecekapan dan kebolehamalian algoritma pengiraan pelbagai pihak. Hasilnya menunjukkan bahawa algoritma bertahan hanya 0.5 saat untuk 1,000 pihak dalam mod luar talian dan 27 minit untuk berjuta peserta dalam mod atas talian.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF ABBREVIATIONS

MPC	-	Multi-party Computation
2PC	-	Two-party Computation
SCET	-	Secure Computing, Economy and Trust
SIMAP	-	Secure Information Management and Processing
SMC	-	Secure Multi-Party Computation
TTP	-	Trusted Third Party
STTP	-	Semi Trusted Third Party
PPCG	-	Privacy Preserving Computational Geometry
PIR	-	Private Information Retrieval
SS	-	Secret Sharing
FIM	-	Frequent Itemset Mining
FIMI	-	Frequent Itemset Mining Implementation
IS	-	Itemset

CHAPTER 1

INTRODUCTION

1.1 Overview

Multi-party Computation (MPC) is a mathematical cryptographic technique that securely computes a function over distributed data among two or more number of parties. It is secure and preserves the privacy of parties' data and does not reveal the sensitive data except the function's result. Multi-party computations use a shared secret which is apportioned among all parties to ensure the privacy of the data. The shared secret guarantees that the function only is computable over all parties. The method of sharing the secret makes the algorithms to behave offline and inappropriate for online problems. In this research, the online secret sharing problem has solved by convergent infinite product sequences. A mathematical fact of the convergent infinite product series has revised to sharing the secret among the parties as the online form. The fact is that the result of the convergent infinite series will be invariant while the number of term increases. The invariant convergence value is used for shared secret, and then each term of the series is used by the parties for sending data. Another problem of online multi-party computation is the information leaking between two consecutive computations, which is solved by two-party computation techniques (Hussein and AlMukhtar, 2009). The proposed innovative online consecutive multi-party computation ensures the security and privacy of all parties' owned sensitive data.

The algorithm is highly practicable for distributed data mining. In fact, today, huge amount of data will be used among the large number of companies. There exist a lot of valuable patterns and roles, which are hidden between voluminous data. Data mining tools have been developed to discover these worth facts. Companies can learn of hidden patterns and rules in their joint databases by using distributed data mining tools to predict the future of their business. While information is distributed between two (or more) companies, and each corporation owns a portion of information, they should collaborate with each other to jointly mine the combined information and find fascinated pattern and rules which are interested by companies. This scenario is known as distributed data mining. It is sophisticated where the data has distributed among the number of parties because of the privacy of their sensitive data. Each company leans to gain the advantage of data mining tools, but it does not propend to share its sensitive data. However, all parties are interested to the result of data mining process over joint databases and would like to participate, but privacy issues may avoid them for exposing their own part of data to other parties. Multi-party computation solves this conflict. The novel proposed algorithm ensures the privacy preserving of data using cryptographic tools as well as precious aggregation over the distributed data.

1.2 Problem Background

The secure multi-party computation also known as (MPC) is one of the principal results of the theory of cryptography. First, Yao (1982) introduced the multi-party computation and nowadays many authors have attended many optimizations and extensions to the basic concept, for two main branches; the two-party (2PC) and the multi-party (MPC) computation (Canetti, 2000; Goldreich, 2004; Goldreich *et al.*, 1987; Jarecki and Shmatikov, 2007; Lindell and Pinkas, 2007; Mohassel and Franklin, 2006; Woodruff, 2007). Most of recent papers on secure multi-party computation area have been focused on theory of multi-party computation and there is no much implementing applicable of MPC, although, in the last few years, some practical implementation of multi-party computation has appeared (Assaf *et al.*, 2008; Bogetoft *et al.*, 2006; Dahlia *et al.*, 2004; Peter *et al.*, 2009; Yehuda *et al.*, 2008).

Secure multi-party computation has divided into two main approaches (Pinkas *et al.*, 2009). The first way is based on arithmetic circuit representation of the computed function and secret sharing, such as in the BGW (Ben-Or, Goldwasser and Wigderson) or CCD (Chaum, Crepeau and Damg°ard) protocols (Chaum *et al.*, 1988; Michael *et al.*, 1988). While most of the participants are trusted (the protocol is not working in two parties case), this method usually applies. Another way is based upon a binary circuit. The approach is designed, especially in the case of original two-party garbled circuit construction of Yao (1986), and in the GMW (Goldreich, Micali and Wigderson) multi-party protocol (Goldreich *et al.*, 1987).

This research is significantly involved with secure multi-party computation algorithms. A secure, applicable and standard offline multi-party aggregation algorithm is developed using ElGamal cryptosystem, due to its simplicity in key management and its homomorphic property. The existing algorithms need to share a secret among all parties; therefore they need to gather all parties before computation starts. Due to secret sharing issue, the current multi-party computation algorithms work at offline mode and the rest are semi-online (Farras and Padro, 2009). There are two main problems to change the offline multi-party computation algorithms to an online mode (Hussein and AlMukhtar, 2009). The first problem is how a secret can be shared online among all parties. The shared secret is usually a calculation of the all parties' keys and therefore, all parties should be present before the process starts to share their secret key. It means that no new party can join the system after the process starts. The offline secret sharing problem avoids the algorithm to apply in online cases, such as online e-voting, e-bidding or web polls.

The second problem is the consecutive computation, which means that some sensitive information reveals by observing the two consequent computation results. In the case of online multi-party computation, if an adversary obtains two consequent computation results, a simple calculation leads to find the *i*th party's private data. The calculation also does not need to decrypt the encrypted posted data, knowledge about the public or private keys, shared secret key or even any collaboration with some parties (Pinkas *et al.*, 2009).

1.3 Problem Statement

This study is intended to come up with an approach to effectively solve the problem of online consecutive multi-party computation algorithm that overcomes the two continuous parties' computation problems. The research question is:

"How to produce the shared secret keys independent from all participants for establishing a secure online consecutive multi-party computation process and avoid the revealing of sensitive data while two continuous parties join the system?"

In order to answer the main issue raised above, the following issues need to be addressed as a prerequisite:

- How the cryptography could synthesize and which cryptography technique is more suitable?
- What is the problem of offline multi-party computation algorithms?
- How do we share the multi-party computation secrets online?
- The main problem will appear in online a case is the 2PC problem. How do we overcome the 2PC problem?
- Whether the proposed algorithm can be combined with data mining techniques?

1.4 Research Goal

The goal of this study is to develop a novel secure, privacy preserver, reliable and online crypto multi-party computation algorithm that can compute an aggregation over distributed data and to ensure that no sensitive information reveals even in the case of 2PC scenario. The minor aim is to apply the innovative algorithm in data mining proposes.

1.5 Research Objectives

In order to achieve the aforementioned aim, listed below are the objectives of this thesis:

- To develop an online secret sharing algorithm based on algebraic infinite convergent series for sharing the multi-party computation secret key in online form.
- To design an online consecutive algorithm that overcomes the leaking sensitive information problem in terms of the continuous computation problem while two incessant parties join.
- To develop distributed frequent itemset mining algorithm using the proposed method for ensuring the applicability of the algorithm and proving the usability of the research.

1.6 Research Scope

Although the potential of multi-party computation for solving many issues is obvious, but there is no much practical application is reported in this area. Secure Multi-Party Computation (SMC) computes the result of function upon the private information of parties with the related environment, ensuring the minimum exposure (Mishra and Chandwani, 2007). SMC provides arguable solutions for organizations for problems like privacy-preserving database query, privacy-preserving scientific computations, privacy preserving intrusion detection and privacy-preserving data mining. Privacy preserving data mining protects the secrecy of raw records while the distributed data mining is processed over aggregate data. The main problem, which is addressed by researchers, is how to mine the accumulated data from different organizations with holding the confidentially of each party. For instance, how two (or more) businesses can discover frequent itemsets among their different databases without revealing their raw records to the others or how an online auction can find the best market clearing price which is equal to best tradeoff between supplies and demands without revealing the customers' online bids or even how a web page can compute the result of the web page poll without revealing visitors' opinion to the web page owner. However, recently, the privacy preserving data mining has attended, but an efficient algorithm for online data mining has not been reported.

While a function computes among some parties online, it means that the result could be computed any time during the process. By this assumption, a foible occurs. If an adversary computes the result of *i*th step and (*i*+1)th step, then the difference between these two values equals to the owned value of the (*i*+1)th person, despite of cryptographic method, without decrypting the values and even without knowledge about the keys. Yao's (1982) secure two-party computation as the seminal in the multi-party computation field is selected as the base of the solution. The online multi-party computation algorithm is combined with a new two-party computation technique for avoiding adversaries to earn sensitive data.

On the other hand, the research scope of database security has expanded greatly, due to the rapid development of the global inter-networked infrastructure. Databases are no longer stand-alone systems that are only accessible to internal users of organizations. Instead, allowing selective access from different security domains has become a must for many business practices. In data mining, the exact values of the data do not important, but a pattern that hides among the data is important. In distributed data mining privacy concern avoids the parties to join to the data mining process. With the above view of multi-party computation, the best solution in the case of distributed data mining is using multi-party computation, which is not considered by researchers. The association rule miming, especially frequent itemset mining is suitable to be implemented by the proposed algorithm. The developed tools have solved the big problem of distributed data mining, and show the practicality of the algorithm, and also emerge the researchers to work more in the new scope known as online distributed data mining using multi-party computation.

1.7 Research Contribution

According to research objectives, the research contributions are listed below;

- Creating the online secret sharing process using convergent infinite product series to produce the online multi-party computation algorithm.
- Improving the online aggregation algorithm using two-party computation techniques and dominate the sensitive information revealing problem.
- Applying the innovative algorithm to data mining tools and ensuring the applicability of the algorithm.

1.8 Research Justification

Although, the multi-party computation was introduced three decades ago by Yao (1982), but few practical applications of multi-party computation is reported. However, the potential of the multi-party computation for solving problems is obvious, but the researchers are not interesting to use multi-party computation in practical applications. It is probably due to the fact that the implementation of the first generation of multi-party computation technique was not enough efficient. Another important factor was poorly understood of the multi-party computation potentials (Peter *et al.*, 2009). Many researchers try to improve the efficiency of the multi-party computation techniques, recently (Damgård and Nielsen, 2003; Damgård and Thorbek, 2007; Gennaro *et al.*, 1998). In the last few years, some practical implementations of multi-party computation have appeared, such as (Amirbekyan and Estivil-Castro, 2007; Bogetoft *et al.*, 2006; Ma and Sivakumar, 2005; Ma and Sivakumar, 2006; Yehuda *et al.*, 2008).

A recent approach is focused on the application of multi-party computation in a range of economic purposes, which are engrossing for practical use (Peter *et al.*, 2009). They have involved in two economic research projects: SCET (Secure

Computing, Economy and Trust) and SIMAP (Secure Information Management and Processing), because of the important role of the trusted third party in the economic research field. The application of multi-party computation is to find the best Market Clearing Price which means the price of per merchandise that is dealt. Suppose that when the price increases, supply will raises and demand will reduces, auctioneer looks for a price where supplies are equal to demands. Secure multi-party computation is employed to hold the privacy of bids that should be computed.

The applicability of multi-party computation which concerned in this research is utilising the multi-party computation in distributed data mining tools. One of the most important tasks in data mining application is mining frequent itemset. These applications include the discovery of association rules, strong rules, correlations, sequential rules, episodes, multi dimensional patterns, and several other important discovery tasks. Association rules are widely used in various areas, such as telecommunication networks, market and risk management, and inventory control. Association rules also are employed, today, in many application areas, including Web usage mining, intrusion detection and bioinformatics. In the case of distributed data, the privacy of sensitive data avoids the miner to find frequent itemsets among the partitioned data.

1.9 Thesis Organisation

The thesis consists of six chapters. Each chapter is briefly described as follows:

- Chapter 1 describes the background, statement of the problem, aim, objectives, research framework, scope, thesis organisation and ends with the thesis contributions.
- Chapter 2 illustrates full literature review of existing methods in offline multi-party computation, and their weaknesses and advantages. The chapter continues with a detail of preliminary requirements cryptographic

techniques and describing the existing distributed data mining tools.

- Chapter 3 briefly describes the research methodology, architecture framework and general overview of the research steps.
- Chapter 4 describes a new proposed online consecutive secure multi-party computation algorithm
    - Section 4.1 starts the chapter with a brief introduction and propounds the main issues.
    - Section 4.2 describes the implementation of the offline aggregation algorithm by ElGamal cryptosystem.
    - Section 4.3 introduces a new online aggregation algorithm that uses an online secret sharing process using the math convergent infinite product series, and its weaknesses and advantages relying on the case studies.
    - Section 4.4 presents the designed online consecutive multi-party computation algorithm that overcomes the new emerged problem known as the 2PC issue.
    - Section 4.5 describes the developed secure distributed frequent itemset mining algorithm using designed method.
- Chapter 5 deals with the applying of novel algorithm in case studies and investigates on experimented results
    - Section 5.1 starts with the explanation of the experimental result environment and technical specifications.
    - Section 5.2 discusses the e-voting process as the selected case study.
    - Section 5.3 deals with the result of the novel proposed algorithm in data mining tools.
- Chapter 6 ends with a conclusion.

REFERENCES

Agrawal, D. and Agrawal, C. (2001). On the design and quantification of privacy preserving data mining algorithms. *Proceedings of 12th ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, 247–255.

Agrawal, D. and Srikant, R. (2000). Privacy preserving mining. *Proceedings of the 2000 ACM SIGMOD Conference on Management of Data*. 439–450.

Agrawal, R., Imielinski, T. and Swami, A. (1993). Mining Association Rules Between Sets of Items in Large Databases. *SIGMOD Conference*, 207-216.

Agrawal, R. and Srikant, R. (2007). Fast algorithms for mining association rules in large databases. *Proceedings of the 33th International Conference on Very Large Data Bases*, pages 487-499.

Aiello, W., Ishai, Y. and Reingold, O. (2001). Priced oblivious transfer: how to sell digital goods. *EUROCRYPT* 119-135.

Amirbekyan, A. and Estivil-Castro, V. (2007). Privacy-Preserving Regression Algorithms. *Proceedings of the 7th WSEAS International Conference on Simulation, Modelling and Optimization*, Beijing, China.

Androulaki, E. and Bellovin, S. (2010). A Secure and Privacy-Preserving Targeted Ad-System. SION, R., CURTMOLA, R., DIETRICH, S., KIAYIAS, A., MIRET, J., SAKO, K. and SEBÉ, F. (eds.). *Financial Cryptography and Data Security.* Springer Berlin / Heidelberg. 6054, 123-135.

Assaf, B.-D., Noam, N. and Benny, P. (2008). FairplayMP: a system for secure multi-party computation. *Proceedings of the 15th ACM conference on Computer and communications security*, Alexandria, Virginia, USA. ACM.

Atallah, M. J. and Du, W. (2001). Privacy-preserving cooperative scientific computations. *14th IEEE Computer Security Foundations Workshop*. 273–282.

Atallah, M. J., Du, W., Dehne, F. K. H. A., Sack, J. R. and Tamassia, R. (2001). Secure multi-party computational geometry. *Lecture Notes in Computer Science, Springer,* 2125**,** 165-179.

Bagüés, S. A., Zeidler, A., Matias, I. R., Klein, C. and Valdivielso, C. F. (2010). Enabling Personal Privacy for Pervasive Computing Environments. *Journal of Universal Computer Science,* 16**,** 341-371.

Baudron, O., Fouque, P. A., Pointcheval, D., Poupard, G. and Stern, J. (2001). Practical Multi-Candidate Election System. *Twentieth Annual ACM Symposium on Principles of Distributed Computing (PODC'01)*. ACM Press, 274-283.

Beaver, D. (1997). Commodity-based cryptography. *twenty-ninth annual ACM symposium on Theory of computing*. 446-455.

Beaver, D. and Goldwasser, S. (1989). Multiparty computation with faulty majority. *Advances in cryptology CRYPTO '89*, New York, NY, USA. Springer-Verlag, 589-590.

Bella, G. (2008). What is Correctness of Security Protocols? *Journal of Universal Computer Science,* 14**,** 2083-2107.

Bertino, E., Fovino, I. N., Parasiliti, L. and Provenza (2005). A Framework for Evaluating Privacy Preserving Data Mining Algorithms*. *Data Min. Knowl. Discov.,* 11**,** 121-154.

Blosser, G. and Zhan, J. (2008). Privacy-Preserving Collaborative E-Voting. *Proceedings of the IEEE ISI 2008 PAISI, PACCF, and SOCO international workshops on Intelligence and Security Informatics*, Taipei, Taiwan. Springer-Verlag, 508-513.

Blundo, C. and Masucci, B. (1999). Randomness in Multi-Secret Sharing Schemes. *Journal of Universal Computer Science,* 5**,** 367--389.

Bogetoft, P., Damgård, I., Jakobsen, T., Nielsen, K., Pagter, J. and Toft, T. (2006). A Practical Implementation of Secure Auctions Based on Multiparty Integer Computation. *Financial Cryptography and Data Security.* 142-147.

Boneh, D. (1998). The decision Diffie-Hellman problem. *Lecture Notes in Computer Science*.

Brassard, G., Cr´epeau, C. and Robert, J. M. (1987). All-or-nothing disclosure of secrets. *Advances in cryptology-CRYPTO '86*, London, UK. Springer-Verlag, 234-238.

Brickell, J. and Shmatikov, V. (2005). Privacy-preserving graph algorithms in the semi-honest model. *ASIACRYPT*, 236-252.

Cachin, C. (1999). Efficient private bidding and auctions with an oblivious third party. *6th ACM conference on Computer and communications security*. 120-127.

Camenisch, J. and Shoup, V. (2003). Practical verifiable encryption and decryption of discrete logarithms. *CRYPTO 2003. LNCS, Springer, Heidelberg,* 2729**,** 126-144.

Canetti, R. (2000). Security and Composition of Multiparty Cryptographic Protocols. *Journal of Cryptology,* 13**,** 143-202.

Canetti, R., Lindell, Y., Ostrovsky, R. and Sahai, A. (2002). Universally composable two-party and multi-party secure computation. *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, Montreal, Quebec, Canada. 509980: ACM, 494-503.

Chaum, D., Crpeau, C. and Ivan, D. (1988). Multiparty unconditionally secure protocols. *Proceedings of the twentieth annual ACM symposium on Theory of computing*, Chicago, Illinois, United States. ACM.

Chen, K. and Liu, L. (2010). Geometric data perturbation for privacy preserving outsourced data mining. *Knowledge and Information Systems***,** 1-39.

Chen, L., Susilo, W., Wang, H., Wong, D. S., Dawson, E., Lai, X., Mambo, M., Miyaji, A., Mu, Y., Pointcheval, D., Preneel, B. and Smart, N. (2008). Cryptography in Computer System Security. *Journal of Universal Computer Science,* 14.

Chiew, K. (2008). Data Mining with Privacy Preserving in Industrial Systems. LIU, Y., SUN, A., LOH, H., LU, W. and LIM, E.-P. (eds.). *Advances of Computational Intelligence in Industrial Systems.* Springer Berlin / Heidelberg. 116, 57-79.

Choi, S., Elbaz, A., Juels, A., Malkin, T. and Yung, M. (2007). Two-Party Computing with Encrypted Data. KUROSAWA, K. (ed.) *Advances in Cryptology – ASIACRYPT 2007.* Springer Berlin / Heidelberg. 4833, 298-314.

Chor, B., Goldwasser, S., Micali, S. and Awerbuch, B. (1985). Verifiable secret sharing and achieving simultaneity in the presence of faults. 26th IEEE Symposium on Foundations of Computer Science. 383-395.

Clifton, C., Kantarcioglu, M. and Vaidya, J. (2002). Defining Privacy for Data Mining. *National Science Foundation Workshop on Next Generation Data Mining*.

Cramer, R., Damgard, I., Dziembowski, S., Hirt, M. and Rabin, T. (1999). Efficient Multi-party Computations Secure Against an Adaptive Adversary. *Advances in Crytology-EUROCRYPT '99,* 1592 of Lecture Notes in Computer Science (LNCS)**,** 311-326.

Cramer, R., Gennaro, R. and Schoenmakers, B. (1997). A Secure and Optimally Efficient Multi-Authority Election Scheme. FUMY, W. (ed.) *Advances in Cryptology — EUROCRYPT '97.* Springer Berlin / Heidelberg. 1233, 103-118.

Dahlia, M., Noam, N., Benny, P. and Yaron, S. (2004). Fairplay;a secure two-party computation system. *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13*, San Diego, CA. USENIX Association.

Damg˚ard, I. and Koprowski, M. (2001). Practical Threshold RSA Signatures Without a Trusted Dealer. *Advances in Cryptology - EUROCRYPT 2001, LNCS, Springer Verlag,* 2045**,** 152-165.

Damgård, I. and Jurik, M. (2001). A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. *Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography*. 746742: Springer-Verlag, 119-136.

Damgard, I., Jurik, M. and Nielsen, J. (2003). A generalization of paillier's public-key system with applications to electronic voting. *special issue of Financial Cryptography, International Journal on Information Security (IJIS)*.

Damgård, I. and Nielsen, J. (2003). Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption. *In Advances in Cryptology - CRYPTO'03*. 2729, 247-264.

Damgård, I. and Thorbek, R. (2007). Non-interactive Proofs for Integer Multiplication. NAOR, M. (ed.) *Advances in Cryptology - EUROCRYPT 2007.* Springer Berlin / Heidelberg. 4515, 412-429.

Das, A. S., Keshri, J. K., Srinathan, K. and Srivastava, V. (2008). Privacy preserving shortest path computation in presence of convex polygonal obstacles. *Third International Conference on Availability, Reliability and Security (ARES '08)*, Washington, DC, USA. IEEE Computer Society, 446–451.

Dasseni, E., Verykios, V. S., Elmagarmid, A. K. and Bertino, E. (2001). Hiding association rules by using confidence and support. *Information Hiding Workshop*, 369–383.

Desmedt, Y. and Frankel, Y. (1990). Threshold Cryptosystems. *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*. 705196: Springer-Verlag, 307-315.

Desmedt, Y. and Frankel, Y. (1994). Perfect Homomorphic Zero-Knowledge Threshold Schemes over any Finite Abelian Group. *SIAM J. Discrete Math,* 7, 667-679.

Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory,* IT-22, 644-654.

Du, W. and Atallah, M. J. (2001). Secure multi-party computation problems and their applications: a review and open problems. *Proceedings of the 2001 workshop on New security paradigms*, Cloudcroft, New Mexico. 508174: ACM, 13-22.

Du, W. and Atallah, M. J. (2002). Privacy-preserving cooperative statistical analysis. *17th Annual Computer Security Applications Conference*. 102–110.

Du, W., Han, Y. S. and Chen, S. (2004). Privacy-Preserving Multivariate Statistical Analysis: Linear Regression and Classification. *Fourth SIAM International Conference on Data Mining*. 222-233.

Du, W. and Zhan, Z. (2002). A practical approach to solve Secure Multi-party Computation problems. *workshop on New security paradigms*. 127-135.

ElGamal, T. (1985). A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory,* 31 469-472.

Estivill-Castro, V. and Brankovic, L. (1999). Data Swapping: Balancing Privacy against Precision in Mining for Logic Rules. *Lectures in Computer Science*.

Even, S., Goldreich, O. and Lempel, A. (1985). A randomized protocol for signing contracts. *Communication ACM,* 28, 637-647.

Evfimievski, A., Srikant, R., Agrawal, D. and Gehrke, J. (2002). Privacy preserving mining of association rules. *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 217–228.

Farras, O. and Padro, C. (2009). Ideal Hierarchical Secret Sharing Schemes. *Cryptology ePrint Archive*.

Fouque, P. A., Poupard, G. and Stern, J. (2001). Sharing Decryption in the Context of Voting or Lotteries. *Financial Cryptography , LNCS, Springer Verlag,* 1962**,** 90-104.

Franklin, M. K. and Reiter, M. K. (1997). Fair exchange with a semi-trusted third party. *4th ACM conference on Computer and communications security*. 1-5.

Frikken, K. B. (2007). Privacy-preserving set union. *ACNS***,** 237-252.

Frikken, K. B. and Atallah, M. J. (2003). Privacy preserving electronic surveillance. *2003 ACM workshop on Privacy in the electronic society*, New York, NY, USA. ACM, 45–52.

Furukawa, J., Miyauchi, H., Mori, K., Obana, S. and Sako, K. (2009). An Implementation of a Universally Verifiable Electronic Voting Scheme Based on Shuffling. BLAZE, M. (ed.) *Financial Cryptography.* Springer Berlin / Heidelberg. 2357, 16-30.

Ge, W., Wang, W., Li, X. and Shi, B. (2005). A Privacy-Preserving Classification Mining AlgorithmThis paper was supported by the National Natural Science Foundation of China (No.69933010, 60303008) and China National 863 High-Tech Projects (No.2002AA4Z3430). HO, T. B., CHEUNG, D. and LIU, H. (eds.). *Advances in Knowledge Discovery and Data Mining.* Springer Berlin / Heidelberg. 3518, 256-261.

Gennaro, R., Rabin, M. O. and Rabin, T. (1998). Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. *Proceedings of the seventeenth annual ACM symposium on Principles of distributed computing*, Puerto Vallarta, Mexico. 277716: ACM, 101-111.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *41st annual ACM symposium on Theory of computing*. 169-178.

Goethals, B., Laur, S., Lipmaa, H. and Mielikainen, T. (2005). On private scalar product computation for privacy-preserving data mining. *7th International Conference on Information Security and Cryptology, Lecture Notes in Computer Science*. 3506, 104-120.

Goldreich, O. (1998). Secure multi party computation. *Working Draft Version,* 1.

Goldreich, O. (2004). *Foundations of Cryptography.* Cambridge Univ. Press.

Goldreich, O. (2005). Foundations of cryptography: a primer Found. *Trends Theor. Comput. Sci.,* 1**,** 1-116.

Goldreich, O. (2008). Encryption Schemes. *working draft.*

Goldreich, O., Micali, S. and Wigderson, A. (1987). How to play ANY mental game. *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, New York, New York, United States. ACM.

Goldreich, O., Micali, S. and Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in NP have zero knowledge proof systems. *JACM,* 38**,** 691–729.

Goldriech, O., Goldwasser, S. and Linial, N. (1991). Fault-Tolerant Computation in the Full Information Model. *32nd IEEE Symposium on Foundations of Computer Science*. 447–457.

Goldwasser, S. (1997). Multi party computations: past and present. *Proceedings of the sixteenth annual ACM symposium on Principles of distributed computing*, Santa Barbara, California, United States. 259405: ACM, 1-6.

Goldwasser, S. and Micali, S. (2006). Probabilistic encryption. *Comput. System Sci*.

Golle, P. and Juels, A. (2008). Dining cryptographers revisited. *Lecture Notes in Computer Science*.

Han, J., Pei, J., Yin, Y. and Mao, R. (2004). Mining frequent patterns without candidate generation. *Data Mining and Knowledge Discovery***,** 53-87.

Hipp, J., Güntzer, U. and Nakhaeizadeh, G. (2005). Algorithms for association rule mining. *SIGKDD Explorations***,** 1-58.

Hirt, M. and Maurer, U. (1997). Complete Characterization of Adversaries Tolerable in Secure Multi-party Computation. *16th Symposium on Principles of Distributed Computing*. ACM Press, 25–34.

Hirt, M. and Maurer, U. (2000). Player simulation and general adversary structures in perfect multiparty computation. *Journal of Cryptology***,** 13:31-60.

Hirt, M. and Sako, K. (2000). Efficient receipt-free voting based on homomorphic encryption. *In Advances in Cryptology - Proceedings of EUROCRYPT* volume 1807 of Lecture Notes in Computer Science.

Hong, J., Kim, J., Kim, J., Franklin, M. and Park, K. (2010). Fair threshold decryption with semi-trusted third parties. *International Journal of Applied Cryptography,* 2**,** 139-153.

Hong, J., Kim, J., Kim, J., Franklin, M. K. and Park, K. (2009). Fair Threshold Decryption with Semi-Trusted Third Parties. *Proceedings of the 14th Australasian Conference on Information Security and Privacy*, Brisbane, Australia. 1574955: Springer-Verlag, 309-326.

Horvitz, O. and Katz, J. (2007). Universally-composable two-party computation in two rounds. *Advances in Cryptology - (CRYPTO 2007)*, 111-129.

Hussein, J. A. and AlMukhtar, M. A. (2009). Fair Exchange of Digital Signatures using RSA-based CEMBS and Offline STTP. *Journal of Computing,* 1**,** 87-91.

Inan, A., Kaya, S. V., SaygIn, Y., Savas, E., Hintoglu, A. A. and Levi, A. (2007). Privacy preserving clustering on horizontally partitioned data. *Data & Knowledge Engineering,* 63**,** 646-666.

Ioannidis, I. and Grama, A. (2003). An efficient protocol for yao's millionaires' problem. *36th Hawaii Internatinal Conference on System Sciences*. 6-9.

Ishai, Y., Prabhakaran, M. and Sahai, A. (2008). Founding Cryptography on Oblivious Transfer – Efficiently. WAGNER, D. (ed.) *Advances in Cryptology – CRYPTO 2008.* Springer Berlin / Heidelberg. 5157, 572-591.

Jain, A. and Hari, C. (2010). A New Efficient Protocol for k-out-of-n Oblivious Transfer. *Cryptologia,* 34**,** 282-290.

Jarecki, S. and Shmatikov, V. (2007). Efficient Two-Party Secure Computation on Committed Inputs. *EUROCRYPT.*

Jing, W., Huang, L., Yao, Y. and Xu, W. (2007). Privacy-preserving statistical quantitative rules mining. *Proceedings of the 2nd international conference on Scalable information systems*, Suzhou, China. 1366892: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 1-2.

Jurik, M. (2003). *Extensions to the Paillier Cryptosystem with Applications to Cryptological Protocols.* University of Aarhus.

Kabir, S. M. A., Youssef, A. M. and Elhakeem, A. K. (2007). On Data Distortion for Privacy Preserving Data Mining. *Canadian Conference on Electrical and Computer Engineering, (CCECE 2007).* Vancouver, BC

Kantarcioglu, M. and Clifton, C. (2002). Privacy preserving distributed mining of association rules on horizontally partitioned data. *ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery***,** 24–31.

Kaya, K., Selçuk, A. and Tezcan, Z. (2006). Threshold Cryptography Based on Asmuth-Bloom Secret Sharing. LEVI, A., SAVAS, E., YENIGÜN, H., BALCISOY, S. and SAYGIN, Y. (eds.). *Computer and Information Sciences.* Springer Berlin / Heidelberg. 4263, 935-942.

Keke, C. (2009). Privacy-Preserving Multiparty Collaborative Mining with Geometric Data Perturbation. *IEEE Transactions on Parallel and Distributed Systems,* 20**,** 1764-1776.

Laur, S. (2004). Special Course on Cryptology: Privacy-Preserving Frequent Itemset Mining on Horizontally Distributed Data. *Institute of Computer Science University of Tartu*.

Laur, S. and Lipmaa, H. (2006). On Security of Sublinear Oblivious Transfer. *Draft*.

Li, C.-T., Hwang, M.-S. and Lai, Y.-C. (2009). *Sixth International Conference on Information Technology: New Generations (ITNG '09)*, Las Vegas, NV 449 - 454

Li, Q., Chan, W. H. and Long, D.-Y. (2010). Semiquantum secret sharing using entangled states. *Physical Review A,* 82**,** 022303.

Lin, H.-Y. and Tzeng, W.-G. (2005). An Efficient Solution to the Millionaires' Problem Based on Homomorphic Encryption. IOANNIDIS, J., KEROMYTIS, A. and YUNG, M. (eds.). *Applied Cryptography and Network Security.* Springer Berlin / Heidelberg. 3531, 97-134.

Lindell, Y. and Pinkas, B. (2000). Privacy preserving data mining. *Advances in Cryptology—Proceedings of CRYPTO 2000 Lecture Notes in Computer Science vol 1880***,** 36–54.

Lindell, Y. and Pinkas, B. (2007). An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries. *EUROCRYPT* 52-79.

Lu, Y. and Desmedt, Y. (2010). Improved Distinguishing Attack on Rabbit. *ISC***,** 17-23.

Luo, H., Zhao, Z. and Lu, Z. M. (2011). Joint secret sharing and data hiding for block truncation coding compressed image transmission. *Inform. Technol. J.,* 10**,** 681-685.

Ma, J. and Sivakumar, K. (2005). Privacy-Preserving Bayesian Network Parameter Learning. *4th WSEAS Int. Conf. on Computational Intelligence, Man-Machine Systems and Cybernetics*, Miami, Florida, USA. 46-51.

Ma, J. and Sivakumar, K. (2006). A Framework of Privacy-Preserving Bayesian Network Parameter Learning using Post Randomization. *WSEAS Transaction of Information Science and Applications,* 3.

Meng-chang, L. and Ning, Z. (2010). A solution to privacy-preserving two-party sign test on vertically partitioned data (P^2 $2NST_v$) using data disguising techniques. *2010 International Conference on Networking and Information Technology (ICNIT)* 11-12 June 2010. 526-534.

Michael, B.-O., Shafi, G. and Avi, W. (1988). Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proceedings of the twentieth annual ACM symposium on Theory of computing*, Chicago, Illinois, United States. ACM.

Mishra, D. K. and Chandwani, M. (2007). Extended Protocol for Secure Multiparty Computation using Ambiguous Identity. *WSEAS Transaction on Computer Research,* 2.

Mohassel, P. and Franklin, M. (2006). Efficiency Tradeoffs for Malicious Two-Party Computation. *Public Key Cryptography - PKC 2006.* 458-473.

Naor, M. and Pinkas, B. (1999). Oblivious Transfer and Polynomial Evaluation. *31st Symp. on Theory of Computer Science (STOC)*, Atlanta, GA. 245-254.

Naor, M. and Pinkas, B. (2001). Efficient Oblivious Transfer Protocols. *SODA 2001 (SIAM Symposium on Discrete Algorithms)*, Washington DC.

Naor, M. and Pinkas, B. (December 2000). Distributed Oblivious Transfer. *Advances in Cryptology -- Asiacrypt '00, LNCS 1976, Springer-Verlag***,** 200-219.

Neff, C. A. (2001). A verifiable secret shuffle and its application to e-voting. *Proceedings of the 8th ACM conference on Computer and Communications Security*, Philadelphia, PA, USA. 502000: ACM, 116-125.

Nielsen, J. and Orlandi, C. (2009). LEGO for Two-Party Secure Computation. REINGOLD, O. (ed.) *Theory of Cryptography.* Springer Berlin / Heidelberg. 5444, 368-386.

Otsuka, A. and Imai, H. (2010). Unconditionally Secure Electronic Voting. CHAUM, D., JAKOBSSON, M., RIVEST, R., RYAN, P., BENALOH, J., KUTYLOWSKI, M. and ADIDA, B. (eds.). *Towards Trustworthy Elections.* Springer Berlin / Heidelberg. 6000, 107-123.

Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. *EUROCRYPT***,** 223-238.

Park, H.-A., Lee, D., Lim, J. and Cho, S. (2007). PPIDS: Privacy Preserving Intrusion Detection System. YANG, C., ZENG, D., CHAU, M., CHANG, K., YANG, Q., CHENG, X., WANG, J., WANG, F.-Y. and CHEN, H. (eds.). *Intelligence and Security Informatics.* Springer Berlin / Heidelberg. 4430, 269-274.

Peng, B., Geng, X. and Zhang, J. (2010). Combined data distortion strategies for privacy-preserving data mining. *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, Chengdu IEEE, 1, 572-576.

Peng, K., Aditya, R., Boyd, C., Dawson, E. and Lee, B. (2005). Multiplicative Homomorphic E-Voting. CANTEAUT, A. and VISWANATHAN, K. (eds.). *Progress in Cryptology - INDOCRYPT 2004.* Springer Berlin / Heidelberg. 3348, 1403-1418.

Peter, B., Dan Lund, C., Ivan, D., rd, Martin, G., Thomas, J., Mikkel, K., igaard, Janus Dam, N., Jesper Buus, N., Kurt, N., Jakob, P., Michael, S. and Tomas, T. (2009). Secure Multiparty Computation Goes Live. *Financial Cryptography and Data Security: 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers.* Springer-Verlag. 325-343.

Pinkas, B., Schneider, T., Smart, N. and Williams, S. (2009). Secure Two-Party Computation Is Practical. *Advances in Cryptology – ASIACRYPT 2009.* 250-267.

Pinto, C. B., Dowsley, R., Morozov, K. and Nascimento, C. A. (2009). Achieving Oblivious Transfer Capacity of Generalized Erasure Channels in the Malicious Model. *Cryptology ePrint Archive*.

Rabin, M. O. (1981). How to exchange secrets by oblivious transfer. *Technical Report TR-81.* Aiken Computation Laboratory, Harvard University.

Rebollo-Monedero, D. and Forne, J. (2010). Optimized Query Forgery for Private Information Retrieval. *IEEE Transactions on Information Theory,* 56**,** 4631 - 4642.

Rivest, R., Shamir, A. and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM,* 21 120-126.

Rizvi, S. J. and Haritsa, J. R. (2002). Maintaining data privacy in association rule mining. *Proceedings of 28th International Conference on Very Large Data Bases***,** 682–693.

Rozenberg, B. and Gudes, E. (2003). privacy preserving frequent item set mining in vertically partitioned databases. *DBSec***,** 91–104.

Saygin, Y., Verykios, V. S. and Elmagarmid, A. K. (2002). Privacy preserving association rule mining. *Research Issues in Data Engineering (RIDE)*, 151–158.

Schaffner, C. (2010). Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Physical Review A,* 82, 032308.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11) 612–613.

Shao, Z. (2010). Fair exchange protocol of Schnorr signatures with semi-trusted adjudicator. *Computers & Electrical Engineering,* 36, 1035-1045.

Shen, Y., Han, J. and Shan, H. (2010). The Research of Privacy-Preserving Clustering Algorithm. *Third International Symposium on Intelligent Information Technology and Security Informatics (IITSI)*, Jinggangshan 324 - 327

Sherman, C., Jie Han, L. and Lakshminarayanan, S. (2009). Two-Party Computation Model for Privacy Preserving Queries over Distributed Databases. *Networks and Distributed Systems Security (NDSS)*.

Stanley, R., Oliveira, M. and Osmar, R. (2002). Privacy preserving frequent itemset mining. *Proceedings of the IEEE international conference on Privacy, security and data mining - Volume 14*, Maebashi City, Japan. Australian Computer Society, Inc.

Tzeng, W.-G. (2002). Efficient 1-Out-n Oblivious Transfer Schemes. NACCACHE, D. and PAILLIER, P. (eds.). *Public Key Cryptography.* Springer Berlin / Heidelberg. 2274, 359-362.

Urabe, S., Wang, J., Kodama, E. and Takata, T. (2007). A High Collusion-Resistant Approach to Distributed Privacy-preserving Data Mining. *IPSJ Digital Courier,* 3, 442-455.

Vaidya, J. and Clifton, C. (2004). Privacy preserving naive Bayes classifier on vertically partitioned data. *In Proceedings of 2004 SIAM International Conference on Data Mining*.

Vanishree, H. and Iyengar, S. R. S. (2009). A novel efficient m-out-of-n oblivious transfer scheme. *IET Seminar Digests,* 2009, 64-64.

Wang, M.-N., Yen, S.-M., Wu, C.-D. and Lin, C.-T. (2006). Cryptanalysis on an Elgamal-like cryptosystem for encrypting large messages. *Proceedings of the*

6th WSEAS International Conference on Applied Informatics and Communications, Elounda, Greece.

Wong, K. S. and Kim, M. H. (2010). Semi-trusted collaborative framework for multi-party computation. *KSII Transactions on Internet and Information Systems,* 4.

Woodruff, D. P. (2007). Revisiting the Efficiency of Malicious Two-Party Computation. *Proceedings of the 26th annual international conference on Advances in Cryptology*, Barcelona, Spain. Springer-Verlag.

Wright, R. (2008). Progress on the PORTIA Project in Privacy Preserving Data Mining. *data surveillance and privacy protection workshop*.

Wright, R. N. and Yang, Z. (2004). Privacy-preserving Bayesian network structure computation on distributed heterogeneous data. *Proceedings of KDD 2004***,** 713–718.

Yang, Z. (2007). *Distributed Protocols for Data Privacy.* Doctor of Philosophy, Stevens Institute of Technology.

Yao, A. C.-C. (1982). Protocols for Secure Computations. *FOCS***,** 160-164.

Yao, A. C.-C. (1986). How to generate and exchange secrets. *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society.

Yehuda, L., Benny, P. and Nigel, P. S. (2008). Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries. *Proceedings of the 6th international conference on Security and Cryptography for Networks*, Amalfi, Italy. Springer-Verlag.

Yu, J. X., Chong, Z., Lu, H., Zhang, Z. and Zhou, A. (2006). A false negative approach to mining frequent itemsets from high speed transactional data streams. *Inform. Sci,* 176**,** 1986-2015.

Zaki, M. J. (2006). Scalable algorithms for association mining. *IEEE Transactions on Knowledge and Data Engineering***,** 372-390.

Zhong and Sheng (2007). Privacy-preserving algorithms for distributed mining of frequent itemsets. *Information Sciences,* 177**,** 490-503.