JAIST Repository
https://dspace.jaist.ac.jp/

Title	プライバシーを保存するいくつかの計算問題への効率的なソリューション
Author(s)	桑，応朋
Citation	
Issue Date	2007-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/3571
Rights	
Description	Supervisor:丹　康雄，情報科学研究科，博士

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

Abstract

In a distributed network, Secure Multiparty Computation (SMC) is always required by the participants who want to compute some functions on their inputs, while ensuring independence of the inputs, correctness of the computation, and that no more information is revealed to a participant other than can be computed from that participant's input and output. In this thesis, we aim at several specific problems in applications of e-bidding, database, and wireless sensor network, all of which belong to the general SMC problem. For these problem, we propose solutions with lower complexities and stronger security than previous results. Specifically, our work is composed of the following four parts:

- We address the problem of Secure Two-party Vector Dominance (STVD) which can be encountered in applications such as multi-commodity private bidding. Alice has a bidding vector $(a_1, ..., a_n)$ and Bob has a price vector $(b_1, ..., b_n)$ for a series of commodities. They would make a deal if there is the dominance relation $\{a_i \geq b_i | i = 1, ..., n\}$, while protecting their privacy on the vectors. Though STVD is a multi-dimensional extension of Yao's millionaire problem which has been extensively researched, it can't be solved by trivially n rounds of a solution for the millionaire problem, because leaking the ordering of each pair (a_i, b_i) to each other is considered a breach of privacy, when there isn't the dominance relation. Till now, previous results on STVD lack strict argument on their correctness, leak sensitive information, or are hard to prevent malicious behaviors. In this thesis we propose an STVD protocol for the semi-honest model, based on an additive homomorphic encryption, and then fix it to be a secure protocol in the malicious model by efficient zero-knowledge proofs. We prove the correctness and security of the two protocols by our formal definitions. The computation and communication cost of the two protocols are $O(nK^2\lambda)$ modular multiplications and $O(nK^2\lambda)$ bits, in which K is the length of each element in the vector, λ is the length of modulus in the encryption scheme. To our knowledge, our work is the first one to efficiently tackle the malicious behaviors in STVD.

- We address the Privacy Preserving Set Intersection (PPSI) problem, in which each party learns no elements other than the intersection of the N private datasets. When datasets are distributed on different sources, finding out their intersection while preserving the privacy of the datasets is a widely required task. We propose an efficient protocol based on a threshold cryptosystem which is additive homomorphic. The protocol is firstly constructed assuming the adversary is semi-honest and controls arbitrary number of parties, then it's extended to resist the malicious behaviors of the adversary. In comparisons with previous results in [36], [62] and [63], our PPSI protocols in the semi-honest and malicious models achieve lower computation and communication costs.

- We address the problem of Privacy Preserving Tuple Matching (PPTM) in a scenario of a horizontally partitioned database among N parties, where each party holds a share of the database's tuples and all tuples have the same set of attributes. Each party wants to determine whether its tuples match those of other parties on all attributes, under the condition that no party publishes its own tuples for privacy concern. We show that another related problem, Privacy Preserving Threshold Attributes Matching (PPTAM), can also be solved by similar techniques. By experiments in a moderate-scale application, our protocol for PPTM saves about 80% computation time in comparison with previous results, with an increase of bandwidth that can be transferred within a few seconds. Though a solution can be derived from the techniques in [62], we are the first to address the PPTAM problem to our knowledge. Our protocol for PPTAM saves about 71.3% computation time and 75% bandwidth in comparison with the derived solution. Both of our protocols are proved to be secure in the semi-honest model.

- We discuss two conflictive privacy issues in pervasive sensor networks, including the originator privacy and sensing area privacy. More and more sensor networks will be deployed in the place where people are living, studying, and working. These sensor networks will bring us the convenience of accessing information anytime and anywhere, whereas put our voice, motion, or even body temperature under surveillance. Under the circumstances of pervasively deployed sensor networks, people will have a dynamic concern about their privacy. At the same time, sensors will become invisible or should be hidden due to the privacy of themselves. We propose a general scheme for people in the environment of pervasive sensor networks, so that they can be aware of whether they should be alert on their privacy activities. Our scheme employs the STVD protocol we achieve in the first part of work as a building block, and has the characteristics of generality and confidentiality.