Form 2

Dissertation Abstract

Report no.	(Course-based) No.1100	Name	Tushar Kanti Saha

Dissertation title	Private computation in the cloud using homomorphic encryption (準同型暗号を利用したクラウド上のプライバシー保護計算)

Abstract

Private computation is the technique of calculating a function with the private inputs from two or more parties. In the modern world, cloud computing has made a revolutionary change in computation process due to the availability of the high-speed Internet everywhere. Now users are interested in outsourcing their large computation to the cloud to save the cost of hardware and software along with their maintenance. At the same time, they want to secure their computation in the cloud. In addition, private computation using homomorphic encryption is a solution to the users to secure data during the computation.

In this thesis, to show private computations in the cloud, we have the following four problems: (i) private multiple queries problem, (ii) private equality tests for single and multiple equalities, (iii) private inequality tests for single and multiple in inequalities, and (iv) private database queries. Moreover, we propose the practical solutions of the mentioned problems whose securities are ensured by somewhat homomorphic encryption based on ring learning with errors in the semi-honest model. In the first problem, we look at secure pattern matching with repetitive wildcards (SPM-RW) which we consider an example private multiple queries problem in the cloud. To solve the first problem, we propose an efficient SPM-RW protocol which outperforms existing technique. To achieve the efficiency, we also propose a data packing method to encode many queries into a single polynomial. In the second problem, we consider two basic sub-problems for equality tests: private equality test (PET) for single equality and private batch equality test (PriBET) for many equalities. To solve the first sub-problem, we propose PET protocol using an existing packing method. To solve the second sub-problem, we propose PriBET protocol using another packing method which is constructed by modifying the packing method of multiple queries. We also divide the third problem into two sub-problems: private inequality test (PIT) for single inequality and private batch inequality test (PriBIT) for many inequalities. Then we show PIT and PriBIT protocols corresponding two sub-problems of inequality tests using some new packing methods to achieve the efficiency. In the fourth problem, we consider four sub-problems in two settings: two-party setting and three-party setting. In two-party setting, we consider private conjunctive, disjunctive, and threshold queries problems. For the conjunctive and disjunctive query problems, we show the solutions using the batch technique of the PriBET protocol. For the threshold query problem, we show the solution using the batch technique of the PriBIT protocol. In three-party setting, we consider a special private conjunctive query (SPCQ) problem with aggregate function. To solve SPCQ problem, we propose SPCQ protocol using another packing method by modifying the packing method of the PriBET protocol to achieve the efficiency. We further show an extension of the PriBET protocol towards big data processing. In addition, our experiments for the mentioned protocols outperform the corresponding state-of-the-art.