氏　　名	KARIN SUMONGKAYOTHIN			
学位の種類	博士(情報科学)			
学位記番号	博情第 370 号			
学位授与年月日	平成 29年 9 月 22 日			
論文題目	Improving bandwidth cost of Oblivious Random Access Machine by using matrix based storage structure （行列型のストレージ構造を使用した ORAM(Oblivious Random Access Machine)の帯域幅コストの改善について）			
論文審査委員	主査	宮地　充子	北陸先端科学技術大学院大学	教授
		金子　峰雄	同	教授
		藤崎　英一郎	同	教授
		面　　和成	筑波大学	准教授
		Steven Gordon	CQU	上級講師
		Komwut Wipusitwarakun	SIIT	准教授

論文の内容の要旨

With the internet technological advances of today, cloud computing is used as a shared pool of computer processing and data for computers and other devices. Since a cloud server is semitrusted, data stored on the server may be secretly investigated for some benefit of the service provider. The cryptography algorithm such as encryption is widely used to ensure the curious server cannot investigate any confidential information of a client. Although the encryption can protect the confidential content from investigating, the curious server still can gain the benefit from other sources of information. Client's behaviour of accessing information is one of the examples which can be investigated. Occasionally, the access pattern or location of data accessed in the storage may leak the information which tells the user's personality.

Oblivious Random Access Machine (ORAM) is known as the algorithm used to hide the clients access pattern from a trusted but curious storage server. Instead of working like a general client-server, ORAM client generates both uploads (write) and download (read) operations whether it wants to download or upload the information. The reason for doing so is to make every access pattern look similar whether upload or download is being performed. In addition, rather than transferring only data of interest, ORAM client transfers group of data in order to hide a data of interest among the other data that are transferred together. According to the processes mentioned earlier, ORAM algorithm incurs of increasing communication overhead, storage overhead, and computation overhead of the system compared to the normal client-server operation. Therefore, the ORAM research focuses on improving the efficiency of the algorithm so that it is able to work as close as the normal system while still maintaining the level of

security as the ORAM should be.

Each different ORAM type has a different design goal, and the protocol used for accessing the information is slightly different depending on the ORAM data structure. However, the common goal for every ORAM researcher is to create the ORAM which is well functional in the practical solution. Typically, the complexity of the ORAM operation is inversely proportional to the size of space requirement on a client. The ORAM which requires the constant storage space of client (e.g. [1] and [2]) needs some extra complex operations to create the security properties, while only few simple operations are enough to a create a secure operation for the ORAM which can provide more extra space on the client (e.g. [3] and [4]). Although an extra space which is required on the client can reduce the complexity of ORAM operation, it does not very beneficial to improve bandwidth consumption spent during the transmission procedure. Since the bandwidth overhead of existing ORAM construction varies according to the ORAM size, bandwidth overhead is another important aspect to be considered besides the operation complexity and storage overhead. In addition, the large storage capacity and high-performance CPUs are generally available at affordable prices. Therefore, the problem of large storage capacity requirement and high complexity of operation is not as important as the use of large amounts of bandwidth for operation. This research focuses on designing ORAM construction which consumes less bandwidth consumption than the other existing schemes while it is still secure under low operation complexity and small storage space usage on the client. To achieve the lower bandwidth consumption than the other ORAM schemes, the new ORAM data structure format should be introduced since the lower bound of bandwidth consumption is based on the ORAM data structure format. In this research, matrix data structure format is used as a basic structure to design the new ORAM construction. It has been named as *Matrix based ORAM*.

Matrix based ORAM is a novel ORAM construction that is implemented based on matrix data structure. Two versions of matrix based ORAM will be introduced in this thesis: Matrix ORAM (M-ORAM) and Recursive Matrix ORAM (RM-ORAM). These two constructions are intended for different uses. M-ORAM is used when the system needs to maximise the efficiency of data transmission while RM-ORAM is suggested to be used when the client has very limited storage capacity. M-ORAM is the first matrix based ORAM construction which has bandwidth overhead dependent from the size of ORAM. Rather than depending on the size of ORAM as other existing ORAM schemes; bandwidth of M-ORAM varies by the height of matrix data structure, thereby allowing M-ORAM to have constant bandwidth cost for any size of ORAM. In addition, M-ORAM uses very simple operation to do an oblivious transfer. It is one of light-weight ORAM schemes that ever have been presented. RM-ORAM, on the other hand, uses slightly complex operations to do the same purpose as M-ORAM. Since RM-ORAM is designed to reduce the use of storage space on the client, it needs some extra operations for transmitting a data to achieve the same security level as M-ORAM. RM-ORAM significantly reduces the client storage usage by using recursion while the computational and bandwidth overhead are slightly increased as a tradeoff.

However, it can achieve better overall asymptotic performance compared with other existing recursive ORAM schemes.

With our two proposed ORAM constructions and their experimental results shown by this thesis, it is evident that the ORAM research has gradually shifted from the theoretical research into practice. It seems likely to be effectively deployed for today's technology.

Keywords: Oblivious Random Machine, Cloud security, Information security, Secure access protocol, Applied cryptography.

論文審査の結果の要旨

Cloud technology is beneficial in many purposes to reduce the cost in IT system infrastructure. The cloud provider can provide the high computational service and huge storage space with the worthy price than the organization will create by their own. These services are shared by many unknown users, and the fact that the cloud provider cannot be fully trusted in the customer's point of view. Oblivious Random Access

Machine(ORAM) is the technique that is used to hide the access pattern and data's address from the untrusted members in the system. To secure access patterns from server's perspective, it incurs of high bandwidth cost, high computation overhead, and extra storage overhead on both client and server. Many ORAMs have been proposed so far try to solve these inefficiencies. They can be categorized into 2 types which are Hierarchical based ORAM and Binary tree based ORAM. Although both ORAM constructions have a different pros and cons, they share the same disadvantage. The disadvantage is when the size of ORAM is increasing, the bandwidth that will be spent for retrieving the information is also increasing.

The aim of this research is to resolve this disadvantades are incurred from ORAM security requirement and solves the problem of growing bandwidth usage when the size of ORAM is increasing. Two ORAM algorithms: Matrix based ORAM (M-ORAM) and Recursive Matrix based ORAM (RM-ORAM) are proposed as our research. M-ORAM achieves constant bandwidth cost for transferring the information under the security requirements of ORAM. Meanwhile, RM-ORAM is designed for constraint storage devices such as IoT or embedded devices. It extremely reduces the space requirement for containing the information on a client without significantly increasing the bandwidth consumption of system. Our innovation has the potential to pave the way for real world ORAM construction which may open the new era of privacy-preserving security solution for cloud services.

As a result, the doctor thesis enhances the security and efficiency of ORAM, which gives incredible impact on the real world. His contribution is exactly enough to get a PhD degree of Information Science.