論文 / 著書情報
Article / Book Information

題目(和文)	分散型秘匿 RAM および秘匿データ構造に関する研究
Title(English)	A Study on Distributed Oblivious RAM and Oblivious Data Structure
著者(和文)	市川敦謙
Author(English)	Atsunori Ichikawa
出典(和文)	学位:博士(工学), 学位授与機関:東京工業大学, 報告番号:甲第12705号, 授与年月日:2024年3月26日, 学位の種別:課程博士, 審査員:尾形 わかは,植松 友彦,山田 功,松本 隆太郎,田中 圭介,安永 憲司
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第12705号, Conferred date:2024/3/26, Degree Type:Course doctor, Examiner:,,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	情報通信 系 情報通信 コース	申請学位（専攻分野）： Academic Degree Requested	博士 (工学) Doctor of
学生氏名： Student's Name	市川 敦謙	審査員主査： Chief Examiner	尾形 わかは

要旨（英文 800 語程度）
Thesis Summary (approx.800 English Words)

Secure multiparty computation (MPC) is a method that enables mutually distrustful parties to jointly compute an arbitrary function over their private inputs. Since breakthrough feasibility results in the 80s, the quest for practically efficient MPC protocols is a central research area in cryptography. Efficiency is measured in terms of computation and/or communication, as a function of the size of the representation of the function that needs to be computed. In the context of MPC, in many cases, that representation of the function is a circuit. This means that, since most of the computation these days is done in RAM programs, RAM-to-circuit transformations are needed in most cases of secure computations.

A distributed oblivious RAM (DORAM) is a method for accessing a secret-shared memory while hiding the accessed locations. DORAMs are the key tool for MPC for RAM programs that avoids expensive RAM-to-circuit transformations, i.e., DORAMs can be used to minimize efficiency losses in secure RAM program computations. This makes MPC more efficient and easier to apply in expensive high-level functions, for example, analytics, machine learning, or data synthesis that involves privacy data. On the other hand, as a primitive closely related to (D)ORAM, Oblivious Priority Queue (OPQ) is also known as a technique that enables to introduce priority queue algorithms into the secure computation. It can be used specifically for certain purposes, e.g., to solve graph-related problems such as a shortest path problem. The OPQs also enables MPC to avoid RAM-to-circuit transformations, not as versatile as (D)ORAMs, but more efficiently in its expertise.

We present new and improved 3-party DORAM protocols. For a logical memory of size N and for each logical operation, our DORAM requires $O(\log N)$ local CPU computation steps. This is known to be asymptotically optimal. Our DORAM satisfies passive security in the honest majority setting. Our technique results with concretely-efficient protocols and does not use expensive cryptography (such as re-randomizable or homomorphic encryption). Specifically, our DORAM is 25X faster than the known most efficient DORAM in the same setting.

Moreover, we extend our technique to handle malicious attackers at the expense of using slightly larger blocks (i.e., $\omega((\lambda + b) \log N)$ vs. $\lambda + b$ where $b = \Omega(\log N)$ is original block size). To the best of our knowledge, this is the first concretely-efficient maliciously secure DORAM. Technically, our construction relies on a novel concretely-efficient 3-party oblivious permutation protocol. We combine it with efficient non-oblivious hashing techniques (i.e., Cuckoo hashing) to get a distributed oblivious hash table. From this, we build a full-fledged DORAM using a distributed variant of the hierarchical approach of Goldreich and Ostrovsky (J. ACM '96). These ideas, and especially the permutation protocol, are of independent interest.

Regarding an OPQ, we construct a novel perfectly secure OPQ that can simulate all PQ functions, inserting an element, extracting the top-priority one, deleting an element, and modifying the priority of an element, in $O(\log^2 N)$ work per query. Our scheme supports the same functions as the state-of-the-art statistical/computational OPQ with higher security, or achieve the same efficiency as the known perfectly secure OPQ with more functions.

備考 ： 論文要旨は、和文 2000 字と英文 300 語を 1 部ずつ提出するか、もしくは英文 800 語を 1 部提出してください。
Note : Thesis Summary should be submitted in either a copy of 2000 Japanese Characters and 300 Words (English) or 1copy of 800 Words (English).

注意：論文要旨は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。
Attention: Thesis Summary will be published on Tokyo Tech Research Repository Website (T2R2).