H-ORAM: A Cacheable ORAM Interface for Efficient I/O Accesses

by

Liang Liu

Bachelor of Engineering, Shanghai Jiao Tong University, 2016

Submitted to the Graduate Faculty of

Swanson School of Engineering in partial fulfillment

of the requirements for the degree of

Master of Science in Electrical Engineering

University of Pittsburgh

2019

UNIVERSITY OF PITTSBURGH

SWANSON SCHOOL OF ENGINEERING

This thesis was presented

by

Liang Liu

It was defended on

March 4, 2019

and approved by

Jun Yang, Ph.D., Professor

Department of Electrical and Computer Engineering

Samuel Dickerson, Ph.D., Assistant Professor

Department of Electrical and Computer Engineering

Jingtong Hu, Ph.D., Assistant Professor

Department of Electrical and Computer Engineering

Thesis Advisor: Jun Yang, Professor, Swanson School of Engineering

H-ORAM: A Cacheable ORAM Interface for Efficient I/O Accesses

Liang Liu, M.S

University of Pittsburgh, 2019

Oblivious RAM (ORAM) is an effective security primitive to prevent access pattern leakage. By adding redundant memory accesses, ORAM prevents attackers from revealing the patterns in the access sequences. However, ORAM tends to introduce a huge degradation on the performance. With growing address space to be protected, ORAM has to store the majority of data in the lower level storage, which further degrades the system performance.

In this paper, we propose Hybrid ORAM (H-ORAM), a novel ORAM primitive to address large performance degradation when overflowing the user data to storage. H-ORAM consists of a batch scheduling scheme for enhancing the memory bandwidth usage, and a novel ORAM interface that returns data without waiting for the I/O access each time. We evaluate H-ORAM on a real machine implementation. The experimental results show that that H-ORAM outperforms the state-of-the-art Path ORAM by 19.8x for a small data set and 22.9x for a large data set.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PREFACE

This thesis is based on the one of my paper work, submitted to the 2019 DAC. By the increasing demand of confidential file transmission, lots of studies developed for the security design. Follow the recommendation from my advisor, Jun Yang, and my supervisor, Rujia Wang, I join the ORAM researching. ORAM is one of the most popular technique defending the side channel attack, and it still has an extremely high potential even after tens of years of study. I am very proud that I can one day participate in developing a new ORAM schemes.

I hereby present my best thanks to my advisor Jun Yang and my supervisor Rujia Wang. We spent 5 months working on this project. The initial idea comes up very quick, only with two weeks, but it turns out that the original design totally does not work. To solve the improper design, we spent about three-month and tried plentiful of methods and finally make it out. During this struggling period, Dr. Yang pointed out several defects and Dr. Wang gave me lots of advices. I could not have this paper without their help.

1.0 INTRODUCTION

A modern cryptography system plays an important role when computing and processing sensitive data. Through years of works, researchers have developed numerous high-performance and secure data encrypt and decrypt techniques. Except the brute force, adversaries can hardly recover the original information only from the captured text.

The trusted hardware, e.g., TPM [3], SGX [7], and XOM [8] secure the processing of sensitive data through data encryption and integrity check, which effectively prevent adversaries from revealing the plaintext or compromising the data. Second paragraph.

However, information may be leaked through various side channels during execution. For instance, the timing information [17], memory access patterns [6] and the power usage [1] are also the accessible sources for the malicious adversaries. By observing or tampering with the sources above, attackers can retrieve sensitive data without directly reading the data contents. For example, researchers have discovered that on a remote data storage server with searchable encryption, access pattern can still leak a significant amount of sensitive information using a little of prior knowledge [6].

Oblivious RAM (ORAM) is a security method primitive initially proposed by Goldreich and Ostrovsky to hide the memory access pattern entirely from adversaries [4]. Several ORAM protocols have been developed since then. They share the same design philosophy: multiple dummy accesses or dummy data blocks need to be padded with actual data access, and the address

needs to be reshuffled periodically to achieve random accesses. The adversaries can only observe a list of memory addresses being accessed, but they cannot correctly guess where the actual sensitive data is. Moreover, since the actual access pattern should be concealed to the malicious adversaries but revealed to the controller, the designer needs a protected area in the hardware to store the essential sensitive information. In the section 2, we will discuss the details of the most representative ORAM schemes.

According to the major invariants of ORAM, to achieve obliviousness, a single data access will couple with tens or hundreds of dummy requests. When the ORAM size is small, the entire ORAM protected data can be entirely loaded into the memory. However, with the increase of data set size, the ORAM capacity will also increase linearly. In such case, the main memory is no longer capable of storing such a large amount of data. Recently, several researchers [2, 13] propose to extent ORAM to the storage level to achieve access pattern protection with larger capacity offered, such that every data request needs to obliviously access both memory and storage, which adds the I/O access overhead to the original ORAM access overhead.

In this paper, we present H-ORAM, a novel hybrid ORAM scheme targets at the slow I/O access bottleneck during ORAM accesses when the ORAM dataset is split in the memory and storage. This work tends to accomplish the following goals while still ensure the security, 1) Construct an ORAM interface with the cache function enabled: the cache is capable of improving the ORAM access time by removing unnecessary I/O accesses, without leaking access pattern by lightweight eviction and shuffle. 2) Decrease the data storage overhead. Our ORAM construction is more compact and uses less space compared to other ORAM protocols. We describe the ORAM background and basics in Section 2, elaborate our motivation in Section 3, describe the details of

our proposed H-ORAM in Section 4. Our theoretical and experimental results are shown in Section 5, and we conclude this paper in Section 6.

2.0 BACKGROUND

2.1 ORAM BASICS

Oblivious RAM protects the system from access pattern leakage by randomly remapping the address after access. In this section, we will briefly introduce the basic concepts of ORAM and then introduce the three classical ORAM schemes, square root ORAM [5, 18], path ORAM [15] and partition ORAM [14]. The square root ORAM is one of the most early proposed ORAM schemes, but it has been gradually abandoned because of its low performance. The path ORAM is the most widely used ORAM, and it is also known as one of the fastest ORAM. The partition ORAM is design for protecting the remote data pattern.

2.1.1 Oblivious Access and Oblivious Store

The basic concepts of ORAM include oblivious access and oblivious store, and all the current ORAM schemes are based on them. The naïve version of oblivious access claims that instead of only accessing the requested one, we should access all sensitive data. Since all the sensitive data have been toughed, the adversaries could hardly guess which one is the real one and the rest ones are dummy. On the other hand, the oblivious store claims that all the sensitive data should be store in a random order, and when accessing each data could only access once. Therefore, even though the adversaries obtain the permuted address it accesses, but they could not guess the actual one, but after a short period of accessing, we should shuffle the whole sensitive data. Both oblivious access and oblivious store are the complete ORAM schemes, and they leak no

information. The drawback is that they consume too much resource. Both oblivious access and oblivious store expand the access overhead from O (1) to O(N). However, the oblivious access and oblivious store define the fundamental protocols, all the following ORAM designs are the combination of them and assemble their own optimizations.

2.1.2 Path ORAM

path ORAM is one of the most simple and practical ORAM protocol, which organizes the memory as a tree-like layout, as shown in Figure 1. Encrypted data can be stored at each node of the tree, and the ORAM controller translates each access into a path access with O(log N) access overhead. After fetching the data inside of the secure ORAM controller, the accessed data will be decrypted and remapped to a different path. Therefore, repeatedly accessing the same data will not reveal the same access pattern on the memory bus. Stash, position map, as well as other components in ORAM controller, need to be stored in securely. Path ORAM requires extra storage space to store dummy blocks, and the best utilization rate is around 50% [15], so storing N real blocks requires 2N space.

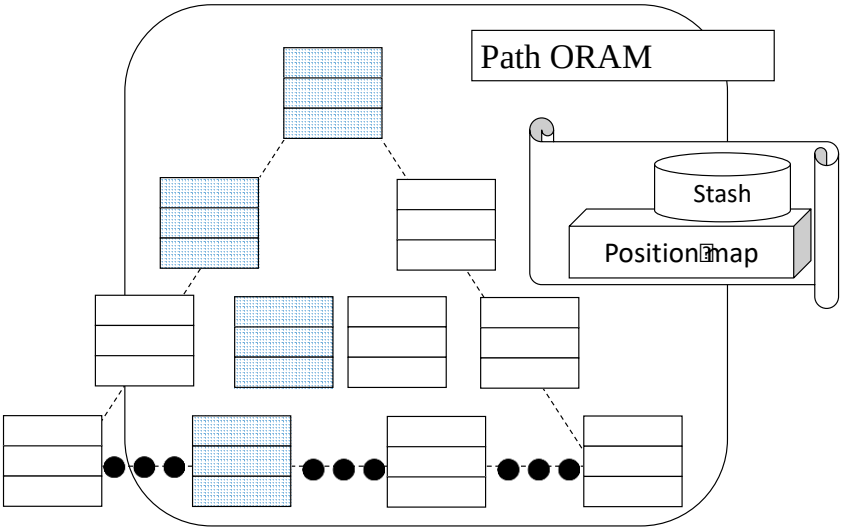


Figure 2-1 Basic Scheme of Path ORAM

2.1.3 Square Root ORAM

A different type of ORAM organizes the memory space as a flat space. Square root ORAM [5, 18] maintains a permutation list which stores the mapping between the physical address and virtual address, as shown in Figure 2. To initiate, N data blocks need to be padded with √N dummy blocks and reshuffled, to generate the permutation list. When a block is not found in the stash, the ORAM controller fetches the data from memory, and when the data is found in the stash, a dummy block also need to be fetched from the memory to avoid information leakage. After T accesses, all dummy blocks in the stash and need to be removed and the whole structure need to be shuffled and re-initialized. Compared with Path ORAM with O (log N) access overhead, square root ORAM requires a O(√ N) of access overhead.

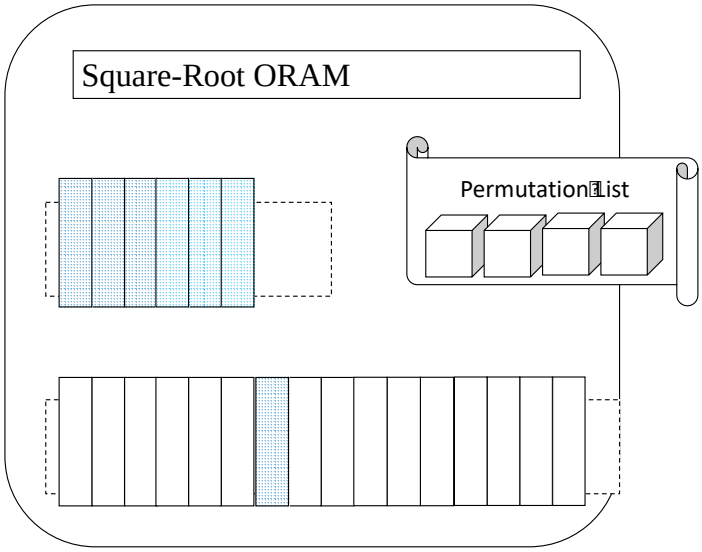


Figure 2-2 Basic Schemes of Square Root ORAM

2.1.4 Partition ORAM

Partition ORAM also uses flat memory organization. Similar to the square root ORAM, each times the partition ORAM fetches one requested block from the database to the stash. The difference of them is that partition modifies the condition to shuffle, and instead of shuffling the whole database, partition ORAM reduce the shuffle overhead each time with more frequent shuffle operations. The partition ORAM divides the database into $\sqrt{N}$ partitions and each partition includes $\sqrt{N}$ blocks. The partition ORAM defines a shuffle period $\{v: v < \sqrt{N}\}$, such that after v blocks of data is loaded to stash, we should evict the stash to memory and conduct a shuffle. The shuffle protocol for partition ORAM is less density, which evicts the *v* blocks of data to a random partition *p*, and only require shuffling the partition *p*.

2.2 THREAT MODEL

Our threat model is similar to most of threat models [11, 12, 14, 16] that need ORAM to protect. We assume that the victim application is safe and the attacker can observe the access pattern of the victim application. We do not consider the side channel information leakage across multiple applications/ users, and the ORAM dataset is private. The application could be run on a computing node with secure hardware such as SGX so that the processor, as well as the on-chip cache, is protected and trusted. Off-chip memory accesses to the protected enclave are encrypted. However, the access pattern may still be observed if the attacker is able to tamper the memory bus. Another scenario is that the application is running on the secure local machine, and it is accessing a remote storage server. The user outsourced data to the cloud storage vendor and the communication (load and store) patterns could leak information.

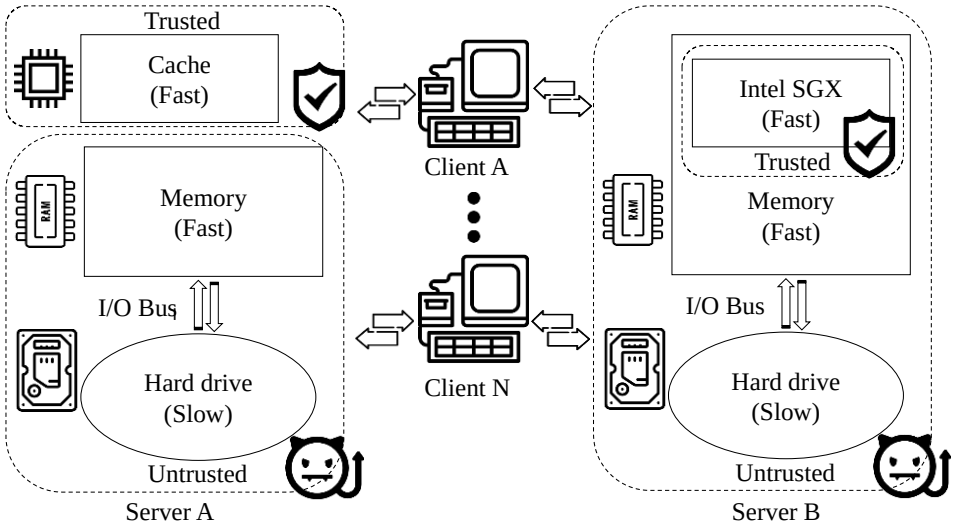


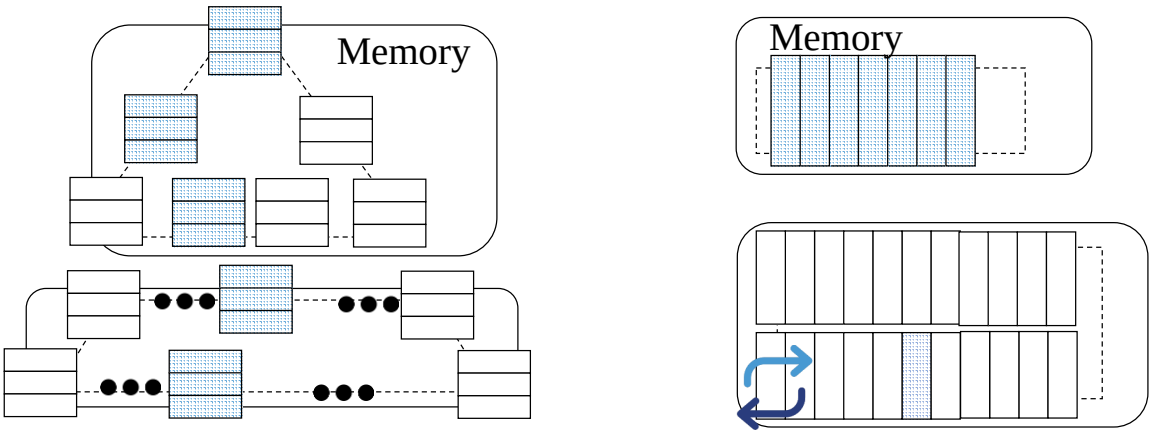
Figure 2-3 Server Setting

3.0 MOTIVATION

3.1 LIMITATIONS OF CURRENT ORAM DESIGNS

Except from the access overhead brought by ORAM protocols, current ORAM designs do not consider the deep memory and storage hierarchy in modern computing systems. For example, in ZeroTrace [13] when the data set is larger than the main memory capacity, they directly extend the leaf nodes to the storage(HDD) backend, as shown in Figure 4 a). The tree-top cache is a straightforward design since most levels are in the fast memory region. However, each path access is translated into multiple fast memory accesses and multiple slow I/O accesses. Also, the tree type organization is hard to adopt other cache techniques because of the low locality. Considering the performance gap between the memory and I/O access, plus the imbalance of memory and I/O usage, such design is inefficient regarding I/O bandwidth overhead.

Using square root ORAM or partition ORAM in such case will reduce the I/O overhead because each time only one data block needs to be fetched from the storage backend, as shown in Figure 4 b). In addition, the flat memory organization allows efficient caching on the top layer. However, the shuffle operation needs to be performed frequently, and the entire storage needs to wait for the shuffle completed before next ORAM operation.



a) Path ORAM with Tree-Top Cache

b) Square-Root ORAM

Figure 3-1 ORAM Schemes with Hardware Setting

3.2 LIMITATIONS OF CURRENT ORAM DESIGNS

The limitations of the existing ORAM protocols motivate us to design a cacheable ORAM interface with low shuffle overhead.

Considering the basic structure of square root ORAM, as is mentioned in Section 2.1, the data is chunk into two parts: stash data and storage data. All data in the stash needs to be accessed when there is an ORAM access, which is an O(√ N) overhead. Accessing the data in the storage only requires a single access, but it needs periodically shuffle. The stash data can be stored in the fast memory, and the memory can use its fast access speed to mitigate the O(√ N) of access overhead, while it only assign a O(1) of tasks to the slow I/O.

However, the results shows that even the fastest memory is hard to afford O(√ N) of redundant accesses. Our first design goal is to minimize the in-memory access overhead while remain the obliviousness. We adopt the Path ORAM for the in-memory data storage, and reduce the overhead from O(√ N) to O(log √N) = O(log N) .

Another inevitable overhead of the square root ORAM is the shuffle process. Unlike the naive shuffle algorithm, ORAM requires an oblivious version of shuffle algorithm such as permutation network, cache Shuffle [9] or Melbourne shuffle [10], all of which bring excessive overhead. Our second design goal is to minimize the shuffle overhead by introducing a new lightweight shuffle process delicately designed for ORAM.

As a result, with the above approaches, our H-ORAM, can theoretically and experimentally outperform the state-of-the-art Path ORAM design in terms of performance and storage overhead. The basic sketch of the H-ORAM memory organization is shown in Figure 5.

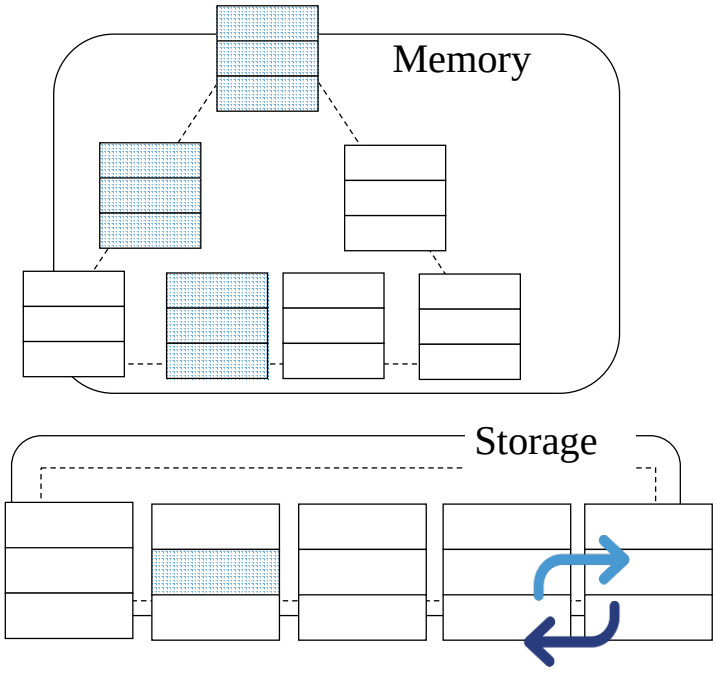


Figure 3-2 Our Proposal H-ORAM

4.0 H-ORAM: DESIGN AND IMPLEMENTATION

4.1 DESIGN LAYOUT AND DATA FLOW

H-ORAM distributes the data to three different physical layers: a control layer, a memory layer, and a storage layer. The first layer is the secure shelter, which utilizes secure hardware such as Intel SGX, and the operations and data inside of the secure shelter are considered tamper-resistant. The second layer in the middle is in memory and it stores data that can be accessed at a high speed. The third layer stores data in the slow but large storage. The design layout of the three layers is shown in Figure 6.

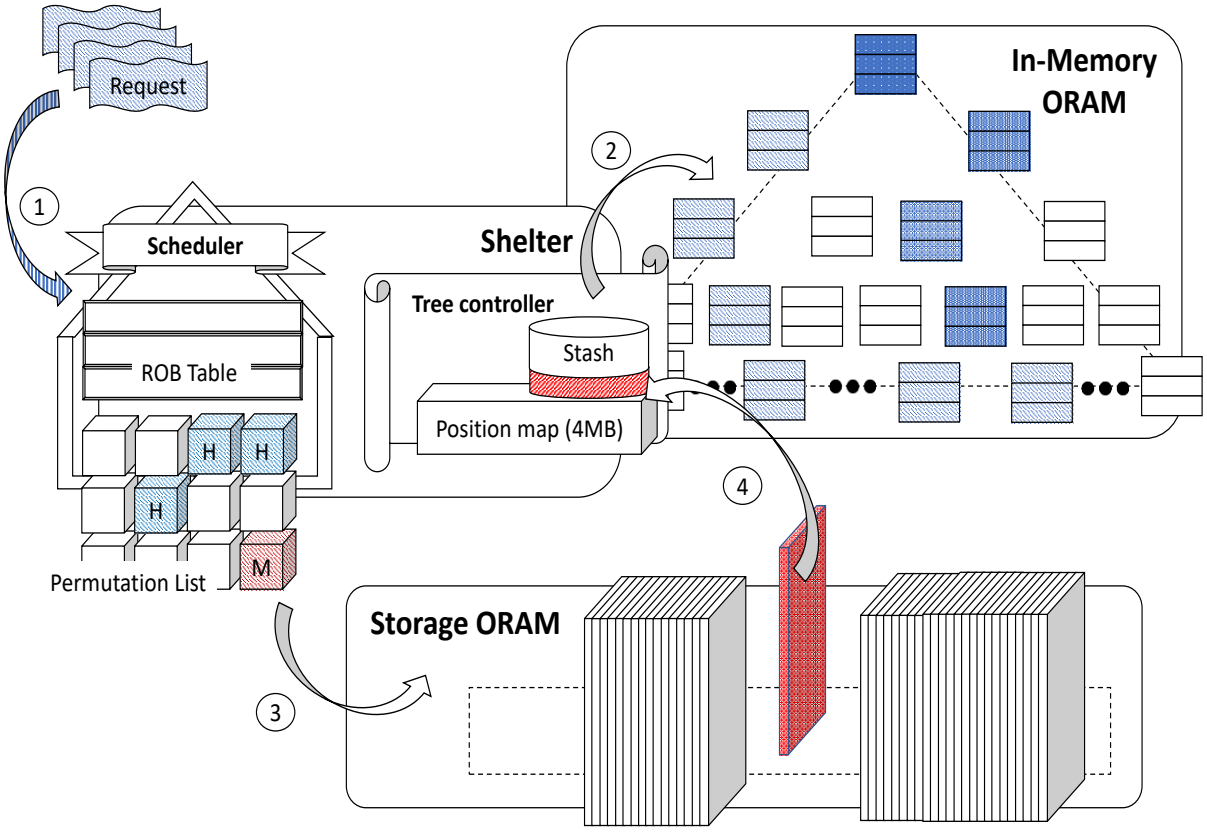


Figure 4-1 Design Layout

4.1.1 Control layer:

The control layer should be protected by the secure hardware. In H-ORAM, the position map for in-memory Path ORAM and the permutation list for storage side ORAM need to be protected. In addition, the control layer contains the scheduler for secure scheduling.

4.1.2 Memory layer:

The data inside is organized as a Path ORAM tree, which can store up to n data blocks (up to 50\% are real blocks). The in-memory ORAM works as the cache during the H-ORAM access. In the beginning, the tree is empty, and data is brought from the storage to the tree. After n/2 blocks have been loaded, the tree is evicted back to the storage and will be reconstructed again.

4.1.3 Storage layer:

The data inside is organized into N data blocks, each of which stores a small, encrypted and permuted data block. To ensure the security, we need to shuffle all the blocks in the storage periodically.

To serve an ORAM request, the scheduler needs to pick and group requests inside of the ROB table. The H-ORAM periodically swaps between two periods: access period and shuffle period. Since the in-memory ORAM can support up to n/2 I/O accesses before next shuffle, we allow n/2 I/O accesses for each access period. For each access, the scheduler will scan the ROB table from the beginning and fetch c requests in the table. (see Section 4.2). Then, the scheduler will firstly check the permutation list for each request. The permutation list records: 1) a Boolean

bit represents whether a block is loaded into memory already, 2) its file address if in storage (or the position map id if in memory). After scanning the ROB table, the scheduler computes 1 I/O address and c in-memory path addresses. The I/O fetches the miss data from the storage to the stash of in-memory path ORAM and assign a random leaf id to it. To utilize the port usage, the I/O loads and in-memory reads are conducted simultaneously. When the group of accesses is finished, the tree access brings the data back to the ROB table, while the I/O access brings data to the stash of the in-memory path ORAM.

When reaching the n/2 limit, the H-ORAM will call the shuffle function. The shuffle period includes three procedures: 1) Evict the path ORAM tree. 2) Shuffle the entire storage data. 3) Initialize a new Path ORAM tree. The detail is shown in the section 4.3.

4.2 SECURE SCHEDULER FOR CACHE PURPOSE

The main reasons that we redesign the square root ORAM is that its structure and its reading strategy is the same as the CPU cache. However, for the ORAM design, we must ensure the security, so we develop a corresponded scheduler scheme. Our scheduler mainly achieves two main functions: one is the grouping strategy and the other is I/O pre-fetching. Our secure scheduler ensures that the hit and miss information for each request keeps unknown for the outside attacker. Therefore, we group multiple requests in to a group that contains similar access pattern. In this section, we introduce the group strategy of scheduler and the I/O pre-fetching to improve the hit rate while remaining the oblivious access pattern.

The scheduler groups every c of the in-coming requests {R1, R2, … Rc} as a group. The c value depends on the hit-rate of the current stage, and our goal is to make that on average in every group, there are c of hit requests and 1 miss. Our scheduler will firstly schedule the I/O load for the miss request, and after the miss request is fetch to memory, we conduct c of in-memory reads for the next cycle.

Since there exist variances among the requests, we cannot exactly find c hit and 1 miss in every cycle, so we have to pad the dummy reads or loads to fill the blank. We further propose an I/O pre-fetching optimization to reduce the dummy requests padded per cycle by early searching next available requests in the ROB table. we define a distance {d: d> c} such that during each I/O cycle, the scheduler will scan the next d requests to find a proper match for the current schedule group.

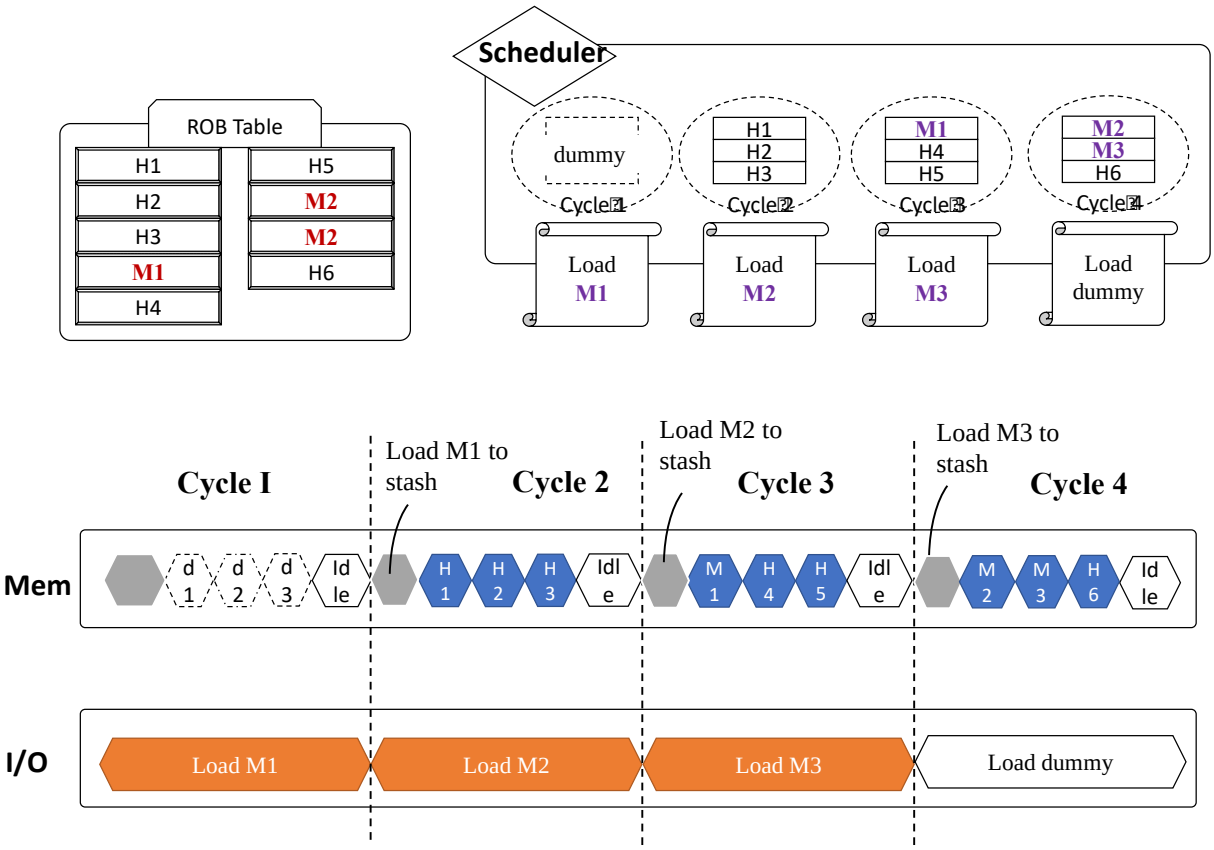


Figure 4-2 An Example of Request Scheduler with Prefetching

Figure 7 shows an example of our group strategy with I/O pre-fetching optimization. In the example, we assume that c=3 and d=9. At the first cycle, the scheduler scans all 9 requests in the queue and schedules the first miss request M1 as a I/O load task. The missed data will then be loaded into the stash and has its path position recorded in the position map. In the second cycle, three hit in-memory Path ORAM read requests {H1, H2, H3} and the next miss M2 are serviced.

After the Cycle 2 is done, the M1 is potentially written back to the in-memory ORAM tree, or still in the stash. Therefore, at Cycle 3, if the M1 is in the ORAM, we read the data as a hit request, and if M1 is in the stash, we read the corresponding path and write M1 back to the in-memory ORAM. The scheduler repeats the same strategy to reorder and group requests, to minimize the number of dummy requests needed per cycle.

Although the hit rate varies across the execution, we use c to represent the average hit rate over a constant period. The whole access period can be divided into s stages, and we use different c value for different stage to evaluate. At the beginning, the in-memory ORAM is empty, so the c is set at a small value. When the in-memory ORAM caches more data, c can be set at a bigger value to issue more in-memory hit requests.

4.3 EVICT AND SHUFFLE

In this section, we discuss how data is managed during the shuffle period of H-ORAM.

4.3.1 Oblivious Tree Evict:

Since the in-memory data tree is exposed to adversaries, when we call the eviction function, we should ensure its obliviousness (without leaking which block is dummy). Here we design a simple approach: 1) Read all the block (both real and dummy) from tree into a temporary buffer. 2) Run the oblivious shuffle on this buffer. 3) Scan the shuffled buffer and remove the dummy. The reorganized evicted data is shown in read in Figure 8.

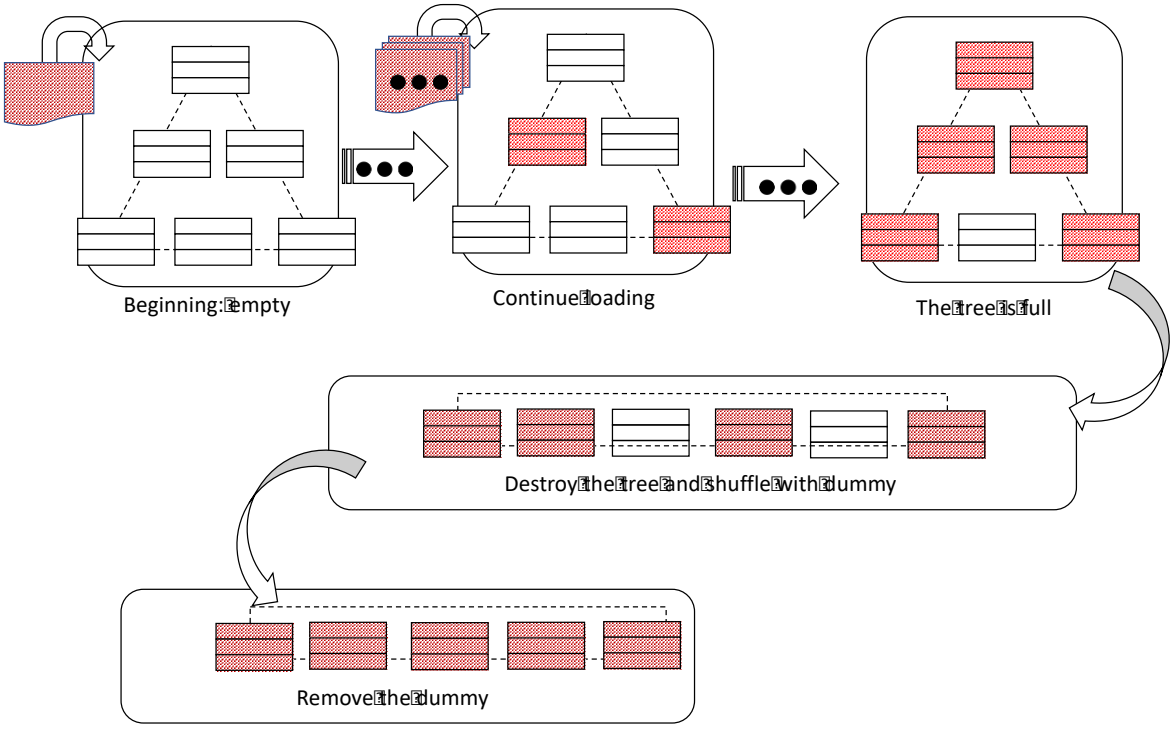


Figure 4-3 Eviction Process

4.3.2 Group and partition shuffle:

The original square root ORAM has an oblivious shuffle stage which brings too much overhead O(4N) of I/O overhead. To reduce the shuffle overhead, we divide the storage into multiple partitions. Similar to the Partition ORAM, we divide the whole data set into √N of partitions and each partition stores √N blocks of data. As is shown in Figure 9, during the shuffle

period, the partitions are shuffled sequentially from the left to right. During the i th shuffle, the controller firstly reads i th partition (cold data) to the memory and concatenates it with the i th pieces of evicted data (hot data) and shuffle them as whole. The in-memory shuffle algorithm is free to choose because memory is fast enough, and we use the cache shuffle here. Finally, we write the shuffled partition to the storage and then process the (i+1) th shuffle.

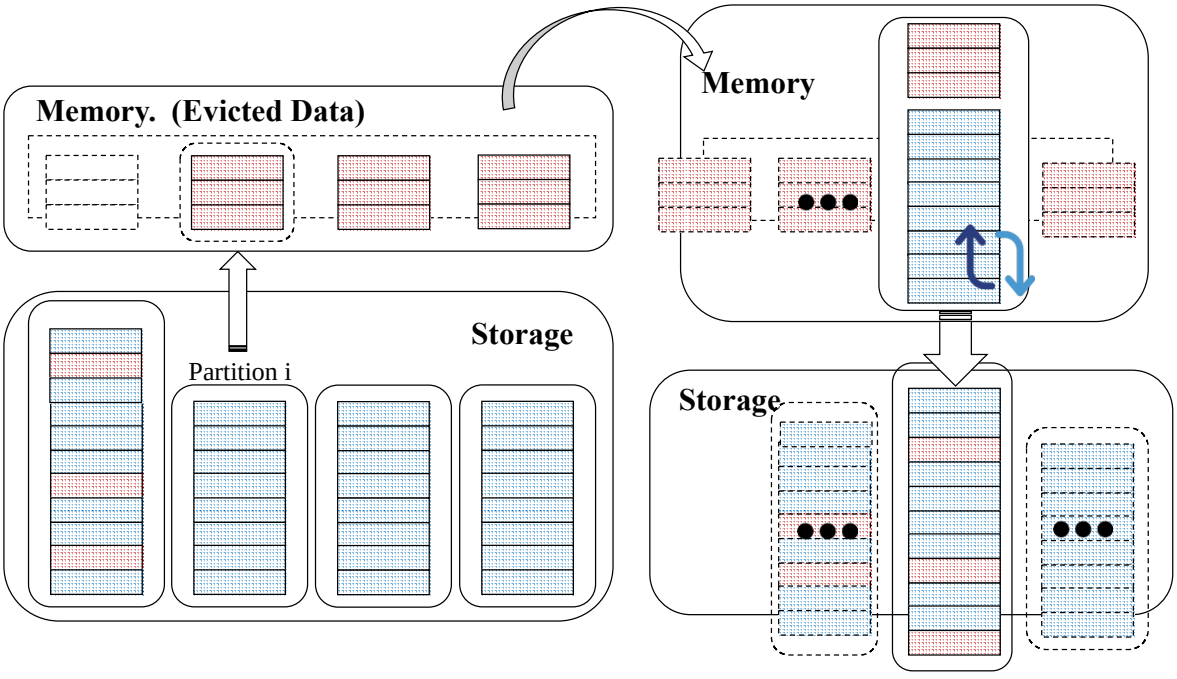


Figure 4-4 Evict and Shuffle Stage of H-ORAM

4.3.3 Security proof:

The different between the proposed group partition shuffle and the partition ORAM is the order of partition to shuffle. We conduct the shuffle from the first partition to the √N partition {1,2, …, √N}. The partition ORAM conduct the shuffle by randomly choosing a partition p, which products a sequence {p1, p2, …, p√N}. However, since both of our H-ORAM and partition ORAM provide the unbiased partition access, which ensure the equivalent possibility of access every partition, which is i \subset {1, 2, …, √N}, P(i) = 1/√N . Therefore, the expect value of i th partition to be shuffle for both schemes are equal. Therefore, our proposed partition shuffle has the equivalent security to the partition ORAM shuffle stage.

4.4 SECURITY ANALYSIS

Our proposed H-ORAM is secure in the following aspects:

4.4.1 Access Security:

The H-ORAM achieves highest security protection when conducting in-memory and I/O access. The in-memory access is protected by path ORAM protocol, which is proof secure by randomly changing the location of data. The data fetch from I/O is shuffled after n accesses, and only accessed once per access period, which is also proof secure by the square root ORAM.

4.4.2 Scheduler Security:

Reviewing from the previous cache design, there is not such an absolutely secure scheduler method to hide the hit or miss information. In this paper, we use the group method to hide the hit or miss information to all parties except the user. However, our design only based on the single user setting, and all the data is requested by the user. Even without leaking, the user can compute hit or miss information from the previous request sequence.

We use the group strategy to hide the hit or miss information to all parties except the user. The adversaries are not able to infer anything from the hit/miss observed on the memory bus, because each scheduling group has the same hit and miss pattern. Reviewing from the previous cache design, there is not such an absolutely secure scheduler method to hide the hit or miss information. In this paper, we use the group method to hide the hit or miss information to all parties except the user. However, our design only based on the single user setting, and all the data is requested by the user. Even without leaking, the user can compute hit or miss information from the previous request sequence.

4.4.3 Shuffle Obliviousness:

In the initial square root requires an oblivious version of shuffle, but the oblivious version of shuffle already exceeds the requirement of ORAM. In the square root ORAM setting, every after a certain period of accessing, the whole dataset should be shuffle. Every data in the storage will only be touched once before shuffle. In addition, both path ORAM and partition ORAM avoid

spending extra in handling cold data, for example, when the path ORAM enter a stable period, the cold data will remain in a certain place and not change frequently.

Our eviction and shuffle ensure the data is periodically permuted in storage. Our design follows the setting of partition ORAM and group the evicted data with cold data in storage into $\sqrt{N}$ for partition shuffle, which achieves the equivalent security of partition ORAM. Instead, the oblivious version of shuffle already exceeds the requirement of ORAM. Both path ORAM and partition ORAM avoid spending extra in handling cold data, for example, when the path ORAM enter a stable period, the cold data will remain in a certain place and not change frequently. Our design follows the setting of partition ORAM (full obliviousness for hot data, half for cold data), and achieve the equivalent security of partition ORAM. As long as no practical attack works for the partition ORAM, our shuffle algorithm is secure.

5.0 RESULTS

5.1 THEORETICAL ANALYSIS

Our baseline is the tree-top-cache path ORAM. In the rest calculation, we denote N as the total amount of block, Z as the bucket size, n/2 as the amount of real block in memory. In section 4.2, we define c as the number of memory requests serviced when waiting for one I/O request. To simplify the process, we compute the average value c, which considers the different execution stages, where ci, ni are the number of the memory requests serviced per stage.1+2s

$$\hat{c} = \frac{2}{n}(c_1 n_1 + c_2 n_2 + \cdots c_s n_s) \tag{5-1}$$

Then, we calculate the I/O overhead of the Path ORAM. Since Path ORAM needs to include dummy data no less than the real data, the total size of baseline Path ORAM to store N real blocks is 2N. Therefore, the path level is calculated as:

$$\text{path level} = \log_2 \frac{n}{Z} + \left(\log_2 \frac{2N}{Z} - \log_2 \frac{n}{Z} \right) = \log_2 \frac{n}{Z} + \log_2 \frac{2N}{n} \tag{5-2}$$

Here, we extract the right most part to calculate the I/O overhead. For the load and store operation, the average I/O overhead of Path ORAM is:

$$Z \log_2 \frac{2N}{n}(reads) + Z \log_2 \frac{2N}{n}(\text{writes}) \quad (5\text{-}3)$$

In comparison, our H-ORAM fetches 1 block each time during the access period. When finishing n c /2 I/O accesses, we need to shuffle the entire dataset. During the shuffle period, H-ORAM fetches (N – n) blocks of data and rewrite N blocks back to storage. Therefore, the average access overhead is:

$$\left\{1 + \frac{2(N-n)}{n\,c}\right\}(reads) + \frac{2N}{n\,c}(writes) \quad (5\text{-}4)$$

In Figure 10, we plot the performance gains of our H-ORAM over the Path ORAM, where the y-axis shows how many times of overhead is reduced and the x-axis represents the N/n ratio (storage size/ memory size). We use a moderate Path ORAM parameter where Z = 4. The result shows that when the ratio is small, the H-ORAM can achieve better performance over Path ORAM. For example, when c = 4, and N/n = 8, we can achieve around 8x I/O access overhead reduction. The best performance is 12 times or 16 times faster than the path ORAM.

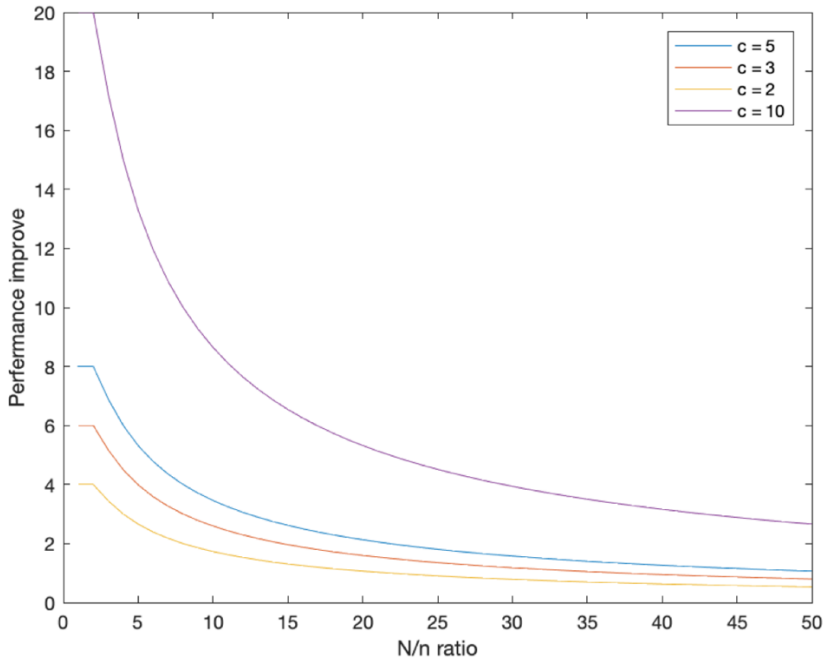


Figure 5-1 Theoretical Performance Gain over Path ORAM

Table 5-1 Overhead Comparison for One Period

	H-ORAM	Path ORAM
Storage/Memory Size	1GB / 128 MB	1.875GB / 128 MB
Path ORAM level	16	16 + 4
Requests Serviced	262144	65536
Access Overhead	1KB (read)	16 KB (read) + 16 KB (write)
Shuffle Overhead	0.875 GB (read) + 1 GB (write)	N/A
Average Overhead	4.5 KB (read) + 4 KB (write)	16 KB (read) + 16 KB (write)

(1 GB data size, 128 MB memory size, 1 KB block siz1 GB data size, 128 MB memory size, 1 KB block size)

Table 1 shows a concrete example that we have a 1GB real data set, and the memory can store up to 128 MB ORAM tree. Follow the previous calculation, for each access period, we can conduct 262,144 I/O requests without shuffle.

$$\frac{n\,c}{2} = \frac{128 \times 1024 \times 4}{2} = 65536 \times 4 = 262144 \tag{5-5}$$

After the 262,144 requests finish, the entire dataset is shuffled (see section 4.3), which brings 1 GB (write) + (1GB - 128 MB) (read) I/O accesses. We calculate the average access overhead as follow:

$$\begin{aligned} \text{average access overhead} &= \text{access overhead} + \frac{shuffle\ overhead}{requests\ serviced} \\ &= 1KB(reads) + \frac{0.875GB\ (reads) + 1GB(writes)}{262144} \\ &= 4.5\ KB\ (reads) + 4KB(writes) \end{aligned} \tag{5-6}$$

Discussion on shuffle overhead: From the above computation, we find that the biggest overhead of our H-ORAM is the shuffle process, since it uses the expensive I/O to read and rewrite the whole data-set. In the practical server setting, there are some opportunities to mitigate the costly shuffle: 1) Perform the shuffle during the off-line time. 2) Considering the client-and-server setting, shown in Figure 11, the shuffle only runs on the remote server, so there is no need to transmit data over the slow network. 3) As shown in our experimental results, the shuffle process consists of sequentially read and write operations, which is 10 times faster than the random data access to the

disk. For the ideal case, without considering the shuffle as an extra overhead, our H-ORAM can theoretically achieve 32 times faster access time than the Path ORAM.

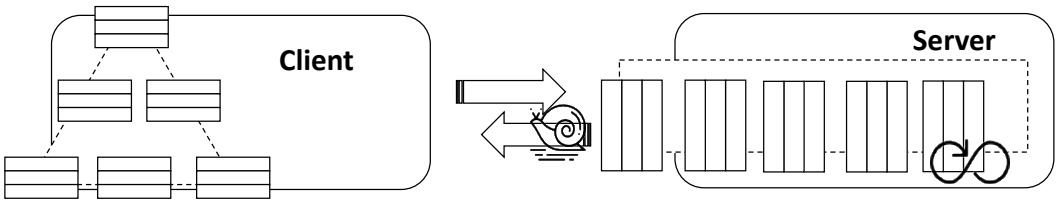


Figure 5-2 Applications of Non-Shuffle Case

5.2 EXPERIMENTAL RESULT

5.2.1 Experiment Setup:

We implement our ORAM interface in a real machine by using the configurations in Table 2. We use HDD as our storage backend, with the average read/write throughput shown below.

Table 5-2 Experimental Machine Setup

Operating System	Linux Ubuntu 16.4
CPU	Intel i7-7700K
Memory	DDR4 Pc4-2133 16 GB
Disk	HDD 7200RPM 500GB
Read/Write Throughput	102.7 MB/s ,55.2 MB/2

We implement Path ORAM and H-ORAM with the naive setting (no recursive). We randomly generate a sequence of requests in which 80\% of chance it will distribute in a certain area, and 20% of chance it requests a random data. During the execution, we divide the access period into 3 stages and set {c1 = 1, c2 = 3, c3 = 5} with number requests per stage {n1 = 0.2, n2 = 0.13, n_3 = 0.67}. On average c = 3.94. We use cache shuffle as the in-memory shuffle algorithm.

We show two sets of results that represent small and large size of data set in Table 3 and 4. The data size is the total ORAM size, but path ORAM needs as twice as the capacity to store the same amount of real data. Both H-ORAM and Path ORAM has same in-memory space.

Table 5-3 64 MB Dataset with 25,000 Requests

	H-ORAM	Path ORAM
Storage/Memory Size	64 MB / 8 MB	120 MB / 8 MB
Number of I/O Access	7228	25000
I/O Latency	77 us	1032 us
Shuffle Time	729 ms * 1	N/A
Total Time	1290 ms	25575 ms

Table 5-4 1 GB Dataset with 500,000 Requests

	H-ORAM	Path ORAM
Storage/Memory Size	1 GB/ 128 MB	1.875 GB / 128 MB
Number of I/O Access	129235	500000
I/O Latency	107 us	1364 us
Shuffle Time	9743 ms * 2	N/A
Total Time	29657 ms	682041 ms

From table 3, the tested HDD has as a read speed twice faster than the write. As the result, the theoretical gains for I/O latency is 4 + 4*2 = 12 times of H-ORAM, which is closed to the measured improvement (13\times).

Because of the cacheable interface, we reduce the required I/O requests for same ORAM access requests. For H-ORAM, only one I/O access is issued per c path ORAM requests. In the small (see Table 3), we tested 25,000 of requests, and the result shows that our cacheable H-ORAM only needs 7,228 I/O accesses to finish all the requests, which is 3.5x reduction compared with the path ORAM. Similarly, for the large dataset test, we achieve 3.8x reduction.

In addition, we observe that the shuffle speed is much faster than the theoretical calculation due to the intrinsic properties of HDD. The access speed is greatly depended on the randomness of requests. When the Path ORAM accessing 4 buckets, it needs to go through 4 sparse locations to fetch the data. For example, {4161, 41090, 114948 ,262665} are 4 bucket addresses when the Path ORAM access the leaf 33289. We observe a large variance between these four addresses, which adds extra overhead when using the HDD. On the other hand, for the H-ORAM, during the

shuffle process, the whole data set is sequentially loaded and written, and it can benefit from the fast-sequential access speed of HDD devices, which is 10xto 20x faster than the random page reading.

5.3 DISCUSSION ON OPTIMIZATION

After years of exploration, numerous of optimization methods have been developed for the Path ORAM and this trend will continue. Our proposed H-ORAM, also assembly the Path ORAM on the top level and optimize the protocol to suit larger data set with a cacheable interface design. The previous studies, that aims at optimizing the position map, stash or tree-top data can also be applied to our H-ORAM. In this section, we discuss a few potential optimizations that can be built on H-ORAM to improve the performance.

5.3.1 Partial shuffle:

As shown in the experimental results, we reduced the ORAM I/O overhead to a minimal amount, but it brings new problem that after the I/O overhead is reduced, the memory become the slower one. Our primary goal is to balance the memory and I/O usage, but this approach fails to achieve a perfect balance. The most significant time spent on H-ORAM, is the shuffle period, which happen every n I/O operation. A full shuffle of entire data is costly. Therefore, we propose a lightweight and flexible partial shuffle protocol. For every shuffle period, we only need to shuffle a portion of the data, for example, r = 1/4 N. Instead of shuffling each partition every period, one partition is going to shuffle every 4 periods. The evicted data from memory keep concatenating on

the top of each partition until 4 periods after last shuffled. With the partial shuffle, we need to issue oblivious access that touches more redundant data each time. The less we shuffle, the more redundant accesses are required. Through this method, we can compute a proper shuffle ratio with a system profiling, which balances the shuffle overhead and the I/O overhead.

5.3.2 Multi-users Case:

Though the Path ORAM has the better performance over the square root ORAM, the square root ORAM has the advantage in the group access, such as the binary search O(N) comparing to the Path ORAM O(N log N) [18]. In the multi-users setting, users might request multiple data at the same time. It can be also regarded as a group data access. Our H-ORAM, as well as square root ORAM, inherently support multiple users to share one ORAM and does not bring extra time for the new coming users. Nonetheless, to ensure security, we need to build a more oblivious scheduler algorithm. When the ORAM protected dataset is shared by multiple users, the system needs to provide high throughput while maintain the obliviousness access between different users. Our proposed H-ORAM groups multiple requests in the scheduler, to maximize the memory bandwidth. When there are multiple users, we can continue to use the group strategy so that requests from different users can be issued at the same time. To protect the access pattern from potential malicious users, some access control protection is required and can be added to our scheduler.

6.0 CONCLUSIONS

Current ORAM designs such as square root ORAM, Path ORAM, face the challenges when the data set grows out of the capacity of main memory. The unavoidable I/O accesses brings extra overhead to the expensive protocols. Meanwhile, it is hard to cache the ORAM accesses because of the unique memory organization. In this work, we propose a novel cacheable ORAM interface, H-ORAM, to reduce the I/O access overhead per ORAM access, and the reshuffle overhead which happens on background. In our theoretical and experimental results, we show that our proposed H-ORAM outperforms the state-of-the-art Path ORAM by 19.8 times for a small data set and 22.9 times for a large data set.

BIBLIOGRAPHY

[1]. Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, and Pankaj Rohatgi. 2002.The EM side channel(s). In International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 29–45.

[2]. Ahmad, A., Kim, K., Sarfaraz, M. I., & Lee, B. (2018). OBLIVIATE: A Data Oblivious File System for Intel SGX.

[3]. Bajikar, S. (2002). Trusted platform module (tpm) based security on notebook pcs-white paper. *Mobile Platforms Group Intel Corporation*, 1-20.

[4]. Goldreich, O. (1987, January). Towards a theory of software protection and simulation by oblivious RAMs. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing* (pp. 182-194). ACM.

[5]. Goldreich, O., & Ostrovsky, R. (1996). Software protection and simulation on oblivious RAMs. *Journal of the ACM (JACM)*, *43*(3), 431-473.

[6]. Islam, M. S., Kuzu, M., & Kantarcioglu, M. (2012, February). Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation. In *Ndss* (Vol. 20, p. 12).

[7]. Johnson, S., Scarlata, V., Rozas, C., Brickell, E., & Mckeen, F. (2016). Intel® Software Guard Extensions: EPID Provisioning and Attestation Services. *White Paper*, *1*, 1-10.

[8]. Lie, D., Thekkath, C., Mitchell, M., Lincoln, P., Boneh, D., Mitchell, J., & Horowitz, M. (2000). Architectural support for copy and tamper resistant software. *ACM SIGPLAN Notices*, *35*(11), 168-177.

[9]. Ohrimenko, O., Goodrich, M. T., Tamassia, R., & Upfal, E. (2014, July). The Melbourne shuffle: Improving oblivious storage in the cloud. In *International Colloquium on Automata, Languages, and Programming* (pp. 556-567). Springer, Berlin, Heidelberg.

[10]. Patel, S., Persiano, G., & Yeo, K. (2017). Cacheshuffle: An oblivious shuffle algorithm using caches. *arXiv preprint arXiv:1705.07069*.

[11]. Ren, L., Fletcher, C. W., Kwon, A., van Dijk, M., & Devadas, S. (2017). Design and implementation of the ascend secure processor. *IEEE Transactions on Dependable and Secure Computing*.

[12]. Wang, R., Zhang, Y., & Yang, J. (2017, February). Cooperative Path-ORAM for effective memory bandwidth sharing in server settings. In *High Performance Computer Architecture (HPCA), 2017 IEEE International Symposium on* (pp. 325-336). IEEE.

[13]. Wang, Z., & Lee, R. B. (2006, December). Covert and side channels due to processor architecture. In *Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual* (pp. 473-482). IEEE.

[14]. Zahur, S., Wang, X., Raykova, M., Gascó n, A.,Doerner, J., Evans, D., & Katz, J. (2016, May). Revisiting square-root ORAM: efficient random access in multi-party computation. In *Security and Privacy (SP), 2016 IEEE Symposium on* (pp. 218-234). IEEE.