

# Panacea: Non-interactive and Stateless Oblivious RAM

Kelong Cong <sup>1</sup>, Debajyoti Das <sup>2</sup>, Georgio Nicolas <sup>2</sup>, and Jeongeun Park <sup>\*</sup><sup>3</sup>

<sup>1</sup> Zama, Paris, France [kelong.cong@zama.ai](mailto:kelong.cong@zama.ai)

<sup>2</sup> COSIC, KU Leuven, Leuven, Belgium. [{debajyoti.das,georgio.nicolas}@esat.kuleuven.be](mailto:{debajyoti.das,georgio.nicolas}@esat.kuleuven.be)

<sup>3</sup> Norwegian University of Science and Technology (NTNU) [jeongeun.park@ntnu.no](mailto:jeongeun.park@ntnu.no)

**Abstract.** Oblivious RAM (ORAM) allows a client to outsource storage to a remote server while hiding the data access pattern from the server. Many ORAM designs have been proposed to reduce the computational overhead and bandwidth blowup for the client. A recent work, Onion Ring ORAM (CCS'19), is able to achieve  $O(1)$  bandwidth blowup in the online phase using fully homomorphic encryption (FHE) techniques, at the cost of a computationally expensive client-side offline phase. Furthermore, such a scheme can be categorized as a stateful construction, meaning that the client has to locally maintain a dynamic state representing the order of remote database elements.

We present Panacea: a novel design of ORAM based on FHE techniques, which is non-interactive and stateless, achieves  $O(1)$  bandwidth blowup, and does not require an expensive offline phase for the client to perform; in that sense, our design is the first of its kind among other ORAM designs. To provide the client with such performance benefits, our design delegates all expensive computation to the resourceful server. We additionally show how to boost the server performance significantly using *probabilistic batch codes* at the cost of only 1.5x in additional bandwidth blowup and 3x expansion in server storage, but less amortized bandwidth. Our experimental results show that our design, with the batching technique, is practical in terms of server computation overhead as well. Specifically, for a database size of  $2^{19}$ , it takes only 1.16 seconds of amortized computation time for a server to respond to a query. As a result of the statelessness and low computational overhead on the client, and reasonable computational overhead on the server, our design is very suitable to be deployed as a cloud-based privacy-preserving storage outsourcing solution with a portable client running on a lightweight device.

## 1 Introduction

Oblivious RAM (ORAM) introduced by [19,20] is a cryptographic primitive which allows a client to store its private data on an untrusted server without leaking any information to the server or any observer about the data or the data access patterns. In that sense, the server would not be able to distinguish which element was accessed by the client nor whether the requested operation was a Read or Write. For efficient *storage outsourcing*, where a client, with limited computational and memory resources wants to store and access some private data on a remote server, an ideal ORAM design should satisfy certain constraints such as low computational, storage and bandwidth overheads when comparing with the plaintext scenario. While the definitions of computational and storage overheads follow directly from intuition, current literature uses *bandwidth blowup* as the metric for measuring overall bandwidth overhead: It is defined as the ratio between the communication cost of ORAM and the non-private case where data travels in the clear. This means that the bandwidth consumed by each client query would be scaled up by a certain factor, relative to the database size. In the classical model of ORAM [22,24,43,44], bandwidth blowup was proven to cost  $\Omega(\log n)$  for a database of  $n$  elements. This is due to restricting the operations of the server to those of a plain storage device which only performs read or write operations, delegating all security and consistency-guaranteeing operations to the client.

---

\* Corresponding author.

This approach is beneficial when deploying ORAM on servers with limited resources, but the bandwidth blowup remains significant as it grows with the database size. To overcome such overheads, many designs have been proposed in the *server computation model* [37,40,39,4,11,18], where parts of the computation are delegated from client to server. Such a model relates more to the current reality of servers being more resourceful than clients: we can safely assume that cloud servers would be able to perform more resource intensive operations than the client due to the difference in available resources. While these designs succeed at reducing some client-side overheads by delegating tasks to the server, most of them still require a bandwidth blowup of  $O(\log n)$ . Moreover, in such schemes, the protocol remains **stateful** and/or **interactive**.

By stateful we mean that the client has to maintain a dynamic state which is mutated when queries are performed to correctly and safely submit subsequent queries. By interactive, we mean that more than one round of client-server interaction is required for the query to be fulfilled. Conversely, a stateless scheme is one where the client only needs to maintain a static state (i.e.: key material, or a hash table), and a non-interactive scheme is one which only requires the client to submit a query and the server to reply with its response in one round-trip for the query to be fulfilled.

Recently, designs based on fully homomorphic encryption (FHE) techniques such as Onion ORAM [12] and Onion Ring ORAM [5] have emerged, achieving a bandwidth blowup of  $O(1)$ . As such, a constant bandwidth blowup decouples the bandwidth complexity from the database size. Nonetheless, these protocols remain stateful and interactive. Despite their low asymptotic guarantees, both of these designs still incur significant overheads on the client: namely in terms of computational, storage and overall bandwidth costs. The construction of Onion ORAM is of purely theoretical interest and remains too costly to implement in practice [23]. The same applies to Onion Ring ORAM, where there exist significant constant factors that are omitted from their complexity claims (See Table 1). Hence, the inability to find a proof of concept implementation that supports the claimed performance metrics due to the large costs in terms computation and memory [5]. Moreover, while claiming non-interactivity in the "online" phase, the latter scheme requires an interactive "offline/eviction" phase to occur periodically at a set number of queries in order to commit writes to the remote database and guarantee security. The bandwidth and computational costs of this eviction phase overshadow any potential client-side advantages gained in the online phase.

Such designs remain stateful as any writes to the database are committed locally in the client's memory until the eviction phase occurs instead of being immediately written on the remote database. The content of the server-side ciphertexts is only updated during initial setup and after each subsequent eviction phase. Thus, if the client requests a read operation targeting an element which they have written to before eviction phases, they would obtain an out-of-date value. This would not be convenient in real world scenarios: if the client loses their internal state but not their keys, they lose all the written but not committed data. For example, in applications such as password managers, it would not make sense to update a password, then have to submit a certain number of queries, and perform eviction before being able to retrieve the new password. In addition, if such a password manager was used on multiple devices, then the client would have to synchronize the dynamic state on all devices after submitting a query from one device.

In that regard, our goal is to build a non-interactive and stateless ORAM scheme which enables us to commit writes to the remote database immediately, without having to "wait" for an eviction

event. This enables client to perform their queries from any device at any point using only static data such as key material or a map of indices which do not need to be updated during queries.

**Our Design.** We propose a novel (single server) ORAM design, which we call Panacea, in the single-server setup. Based on fully homomorphic encryption (FHE) techniques, Panacea achieves  $O(1)$  bandwidth blowup (equivalently  $O(\log n)$  communication complexity) and low client-side computational overhead by pushing almost all of the required computation server-side: The client only needs to encrypt the queries it submits to the server and decrypt responses upon reception; and thus does not need to take part in any expensive offline phase, or extra interaction emulating a plaintext storage solution.

*Core Design Strategy.* We employ a technique called *homomorphic de-multiplexing* (adapted from [10]) which allows the server to operate on all elements in a database while obliviously retrieving the client-indexed element. In that sense, Panacea introduces a completely new technique for ORAM protocol design. A tool which we hope would be useful in building new privacy-preserving technologies.

We present three variants of Panacea: the first version implements the above idea directly, optimizing the number of bits required to represent an address and the total amount of computation required by the server. In contrast to Onion Ring ORAM or Path ORAM [38], we rely on a linear database structure, just like standard RAM. This does not require the client to maintain a representative state to figure out where each element would be located. This enables our client to be stateless, and allows our scheme to be easily composable and deployable as will be demonstrated in the next variants. With such a stateless design, the client can query the server, go offline, and then retrieve the results whenever it comes back online. Another notable advantage is that the client can use its key to access the database from multiple devices without the need for state synchronization, similar to the advantages of stateless digital signatures when compared to stateful digital signatures. However, achieving a stateless and non-interactive client with a constant bandwidth blowup comes at a cost: operating on all elements of the database requires a computational overhead of  $O(n)$  on the server for a database size of  $n$ . We acknowledge that this is suboptimal, but believe that this is a compromise worth conceding in order to enable novel privacy-preserving applications. In our two variants of the main protocol, we employ amortization techniques that render our server performance more practical in certain use-cases.

*Optimization Method 1.* Our first optimization method leverages the highly parallelizable nature of the linear database structure we employ. Given that the order of execution of operations on a linear database would not impact the final output, we can reduce the time needed for the processing of a batch of  $k$  queries on distinct elements. This can be made possible by parallelizing the homomorphic de-multiplexing operations using multiple threads. Thus the server now needs to operate on each database element only once (instead of  $k$  times) for a batch. The asymptotic computation overhead for the server still remains  $O(n)$ .

*Optimization Method 2: Using Batching.* Our second version leverages existing batching techniques from the literature to amortize the server’s computational cost for a batch of  $k$  queries at the expense of adding some bandwidth blowup. More specifically, we use an existing technique called probabilistic batch codes (PBC) which incur 1.5x of additional (total) bandwidth and increase the database size by 3x in our settings, but the amortized bandwidth decreases as the size of batch increases (See Section 6). PBCs also introduce a very small failure probability of one-in-a-trillion. In this context, a failure translates to only some (but not all) of the  $k$  read/write queries being executed. Nonetheless, such a failure does not leak any information to the server. PBCs are

traditionally used for load-balancing applications and private information retrieval (PIR) schemes such as [2], and cannot be directly applied to an encrypted non-static database because mutating individual elements would cause consistency issues in the PBC encoding. We solve this problem using our *consistency correction* technique. To the best of our knowledge, this is the first time that PBCs are applied to an encrypted, non-static database. The asymptotic computational complexity for the server is  $O(n/k)$  when PBC is employed.

While the server computation overhead of Panacea is asymptotically higher compared to that of the existing stateful designs [5,38], we give concrete and reproducible performance results on databases with up to  $2^{19}$  data elements and show that our construction is more practical and scalable compared to theirs when deploying on the cloud: we achieve around 1.16 seconds of amortized computation time for the server to respond to a query, and a bandwidth blowup of 8 for the client (Onion Ring Oram and Path Oram incur bandwidth blowups of 12.8 and 160 respectively). To summarize our contributions:

1. we present a novel ORAM design, where a client can be stateless, based on the homomorphic de-multiplexer technique (§4).
2. we show performance optimizations for a batch of  $k$  queries:
  - (a) Our first technique utilizes parallel threads, and optimizes the number of operations executed by the server (§5).
  - (b) Our second technique uses batching techniques from literature in combination with our consistency correction algorithm to make the server-side computational cost practical (§6).
3. we implement and evaluate the performance of our core design along with the batching technique and describe a cloud-based deployment strategy for performance optimization (§7).

## 2 Background and Related Work

### 2.1 ORAM Syntax

We consider a single-server ORAM setup where a client wants to outsource the storage of its private data to an untrusted server. For a single query, the ORAM algorithm provides an **Access** function to the client which takes as input a 3-tuple  $(a, \text{op}, \text{data})$ , where:

- $a$  represents the logical address of the block requested by the client;
- $\text{op} \in \{\text{Read}, \text{Write}\}$ ;
- $\text{data}$  is the data being written to the block if  $\text{op} = \text{Write}$  (if  $\text{op} = \text{Read}$  the block is not updated and  $\text{data}$  is ignored).

The goal of the ORAM algorithm is to completely hide the data access pattern (which blocks were read from/written to) from the server. We consider that the client fetches/stores data on the server in *blocks*. A typical block size for cloud storage could be range from a few to several hundred KB. We consider that the database contains  $n$  distinct data blocks that are stored on the server. All relevant notations are summarized in Table 2.

**Threat Model** We consider an honest-but-curious server, i.e., the server follows the prescribed protocol correctly. However, the server may store all ciphertexts and metadata transmitted by the client then, afterwards, act as a probabilistic polynomial time adversary to perform additional computations in order to infer information regarding the database contents or the access pattern of the client. We adopt a standard security definition similar to [40,35].

**Definition 1** (Security). Let  $\mathbf{y} := \{(a_1, \text{op}_1, \text{data}_1), \dots, (a_s, \text{op}_s, \text{data}_s)\}$  denote a sequence of data accesses by the client, where  $a_i$  denotes the address of the block being read from or written to on the  $i$ -th access,  $\text{op}_i$  denotes the whether the operation on  $a_i$  is a read or write,  $\text{data}_i$  denotes the data if the  $i$ -th operation is a write operation. Let  $A(\mathbf{y})$  denote the sequence of communication between the client and the server under an ORAM protocol  $\Pi$  for the access sequence  $\mathbf{y}$ . We say that  $\Pi$  provides security with correctness parameter  $\mu$ , if the following properties hold:

- **privacy:** for any chosen pair of data access sequences  $\mathbf{y}$  and  $\mathbf{y}'$  of same length, the server cannot computationally distinguish between  $A(\mathbf{y})$  and  $A(\mathbf{y}')$ ;
- **correctness:** for a sequence of input  $\mathbf{y}$ , the protocol returns output to the client consistent with  $\mathbf{y}$  with probability greater than  $1 - \mu$ .

Ideally, we want to minimize  $\mu$  as much as possible: if some elements of the returned output is not correct, the client could query those elements again as long as the inconsistencies can be detected. Similar to other works, we do not consider leakage through side channels such as when or how frequently the client queries the ORAM. We briefly discuss achieving integrity against a potentially malicious server in Appendix A.4, based on existing techniques from the literature.

## 2.2 System Goals

In order to support the cloud storage scenario where the same user can have multiple client devices, possibly with low processing power and storage capacity, to access the same database, we aim to achieve the following system goals:

- **Statelessness:** the client should not have to maintain and continuously update any state related to the database, except for key material used to encrypt or decrypt the elements. This will also allow the ORAM protocol to be operational even if a client device crashes or reboots.
- **Non-Interactivity:** the client should not have to participate in the protocol interactively; it should be able to construct the query, submit it to the remote server, go offline, then retrieve the response whenever it comes online. The response does not have to be retrieved by the same device from which the query was submitted.
- **Medium Scalability:** we aim to scale efficiently for moderately-sized databases of a few hundred thousands elements. So we pick database size of  $2^{19} \approx 500K$ .<sup>4</sup>
- **Minimal Bandwidth Blowup:** we aim to achieve  $O(1)$  bandwidth blowup to support resource-limited clients.

## 2.3 Existing ORAM Designs

ORAM was first introduced by Goldreich and Ostrovsky in their seminal work [21], where they prove that ORAM designs in the classical model has a fundamental requirement of  $\Omega(\log n)$  bandwidth blowup. Path ORAM [38] is a prominent example in this line of work which achieves a bandwidth blowup of  $O(\log n)$  by utilizing a binary tree-based database structure. However, due to the inherent regular mutations to the structure of binary trees, the client in Path ORAM is required to locally maintain a representative state of the database’s structure to be able to keep track of the location of each data element; which implies a stateful client with memory overhead.

<sup>4</sup> 500K is approximately the total number of full-text articles in ACM digital library as of the moment of redaction.

Table 1: Comparison between our design and previous ORAM approaches in terms of storage requirement (in bits) of both server and client, and computation complexity for a batch of  $k$  queries. We denote  $L$  as the number of levels of ORAM tree of Onion Ring ORAM [5] and Path ORAM [38],  $Z$  as the number of slots in each node, set as  $2^9$  in practice,  $n$  the number of data elements, and  $N$  and  $q$  as ciphertext parameters of underlying FHE scheme.  $w$  is the number of hash functions used for our batching technique. In our work we set  $w = 3$ .

	Ours (Method 1)	Ours (Method 2)	Onion Ring ORAM [5]	Path ORAM [38]
Memory (Server)	$O(n \cdot N \cdot \log q)$	$O(w \cdot n \cdot N \cdot \log q)$	$O(Z \cdot (2^L - 1) \cdot N \cdot \log q)$	$Z \cdot n$
Memory (Client)	$O(1)$	$O(w \cdot n \cdot \log n)$	$O(n \cdot \log n + Z \cdot N \cdot \log q)$	$O(\log n) \cdot \omega(1)$
Stateful	×	×	✓	✓
Interaction with Client	×	×	✓	✓
Computation (Client-Query)	$O(k \cdot \log n)$	$O(k \cdot \log n)$	$O(k \cdot \log n)$	$O(k \cdot \log n)$
Computation (Client-Eviction)	×	×	$O(Z \cdot \log Z \cdot \log n)$	$O(k \cdot \log n)$
Amortized Computation (Server)	$O(n)$	$O(\frac{w \cdot n}{k})$	$O(\frac{Z \cdot \log Z \cdot \log n}{k})$	$O(\log n)$

To circumvent the lower bound set by Goldreich and Ostrovsky, many ORAM designs were proposed in the server computation model [37,40,39,4,11,18,41]. In the server computation model, the server does not just act as a plain storage device. Instead, it helps in offsetting the cost of bandwidth blowup and client-side computations by performing additional expensive computations compared to the case in the classical model. However, most of these designs cannot reduce the bandwidth blowup to less than  $O(\log n)$ . It is only until recently that the designs of Onion ORAM and Onion Ring ORAM have been capable to circumvent the  $O(\log n)$  bandwidth blowup. Using FHE techniques, both designs provide a non-interactive online phase with a bandwidth blowup of  $O(1)$ . However, given that they both employ binary tree-based database structures, similar to Path ORAM, their clients need to maintain a state of the database’s structure locally. Additionally, Onion ORAM and Onion Ring ORAM introduce expensive interactive eviction (offline) phases to achieve their guarantees. While Onion Ring ORAM brings forward improvements over Onion ORAM, it nevertheless still incurs significant computation and memory overheads on the stateful client: the client is required to perform expensive operations and interact with the server during the eviction phase.

We observe that such binary tree-based structures are not a necessity when using FHE techniques: the server can operate on all elements while reading from/writing to only one element, or a batch of them at a time. This motivates us to take a step away from this design paradigm, and propose a novel design strategy which achieves a non-interactive and stateless client for the ORAM scheme while guaranteeing a bandwidth blowup of  $O(1)$  and eliminating the need for offline eviction phases.

A stateless ORAM can be built by combining PIR and PIR-write [26] which only supports “write” operations as [31] have pointed out. However, the state-of-the art PIR-write [42] still incurs a computational complexity of  $O(n \log n)$ . Our writing part, named **update phase**, can be considered as PIR-write with optimal bandwidth:  $O(\log n)$ , and optimal computational complexity:  $O(n)$ .

*Other Interesting Designs.* Using the technique of Recursive ORAM [21], a design can achieve statelessness by recursively storing the state of the database as another ORAM on the same server. However, such designs require  $O(\log n)$  client-server interactions to achieve an overall bandwidth blowup of  $\Omega(\log n)$ . The design of TWORAM [16] avoids such the need for recursive interactions by employing garbled circuits to access data elements, and using the output of the garbled circuit as

Table 2: Protocol and system parameters for ORAM

$DB$	The database
$n$	Number of data blocks (elements) in $DB$
$w$	Number of hash functions for PBC
$k$	Number of queries in a single batch query
$b$	Number of buckets in $DB$ to support PBC
$p$	Failure probability of PBC
$op$	The access type, $op \in \{\text{Read}, \text{Write}\}$
$\langle \mathbf{v}, \mathbf{w} \rangle$	Dot product of two vectors $\mathbf{v}, \mathbf{w}$
$\mathbf{x}_i, \mathbf{x}[i]$	The $i$ -th component of vector $\mathbf{x}$
$\log(\cdot)$	Logarithm function with base 2
$N$	The maximum degree of a polynomial
$t$	Plaintext modulus
$q$	Ciphertext modulus
$\ell$	Decomposition parameter
$\mathcal{R}$	$\mathbb{Z}[X]/(X^N + 1), N \in \mathbb{N}$
$\mathcal{R}_q$	$\mathbb{Z}[X]/(X^N + 1) \bmod q, q, N \in \mathbb{N}$
$\lambda$	Security parameter

the input to the next access recursively. However, this would require the client to update the garbled circuits for the accessed elements after every access: which actually increases the overall bandwidth overhead and without decreasing the blowup from  $\Omega(\log(n))$ , and brings back the requirement of secure client-side storage.

There exist ORAM designs in the multi-server model [25]. However, they inherently aim for a weaker adversarial setting by requiring a subset of those servers to be honest.

### 3 Preliminaries

#### 3.1 Preliminaries of Underlying FHE Scheme

Our protocol, introduced in the next section, can be instantiated with any IND-CPA secure FHE scheme. However, for efficiency, we specifically chose a scheme which is secure based on the (R)LWE problem [34,30], and supports efficient homomorphic operations. Therefore, we define our ciphertexts and basic homomorphic operations over them, which will be used in our instantiation.

**Notations.** We summarize our notations in Table 2.

**Ciphertexts** We define the ciphertext modulus as  $q$  and the plaintext modulus as  $t$ , where  $t \ll q$ , and denote  $\Delta = \lfloor q/t \rfloor$ .

- An RLWE ciphertext is defined as  $c := (a, b) \in \mathcal{R}_q^2$ , where  $b = a \cdot s + \Delta \cdot m + e$  for a message polynomial  $m \in \mathcal{R}_t$  and a secret key  $s \in \mathcal{R}$ .  $c$  is denoted by  $\text{RLWE}_s(m)$ .
- Given a base  $g$  and  $\ell = O(\log q)$ , we define a gadget vector  $\mathbf{g} = (1, g, \dots, g^{\ell-1})^t$ . An RGSW ciphertext is a form of  $\mathbf{C} := (\mathbf{a}, \mathbf{b}) \in \mathcal{R}_q^{2\ell \times 2}$ , where  $\mathbf{b} = \mathbf{H} + m \cdot \mathbf{G}$ , where each row of  $\mathbf{H}$  is an  $\text{RLWE}_s(0)$  and  $\mathbf{G}$  is a gadget matrix which is defined by  $\mathbf{G} = \mathbf{I}_2 \otimes \mathbf{g}$ . The ciphertext is denoted as  $\text{RGSW}_s(m)$ .  $s$  can be omitted if it is clear from the context.

**Homomorphic Operations and Basic Algorithms** *Homomorphic Addition.* Let  $c_1 := (a_1, b_1)$  and  $c_2 := (a_2, b_2)$  be two RLWE ciphertexts. The addition between two ciphertexts is defined as  $c_+ := c_1 + c_2 = (a_1 + a_2, b_1 + b_2)$ .

*External Product.* We denote a homomorphic multiplication between an RLWE ciphertext and an RGSW ciphertext as  $\square$ , which is called external product in [7], and define it as follows:  $a \square \mathbf{B} = \mathbf{G}^{-1}(a) \cdot \mathbf{B}$ , where  $\mathbf{B}$  is an RGSW( $m_B$ ) where  $B \in \{0, 1\}$  and  $a$  is an RLWE( $m_a$ ) where  $m_a \in \mathcal{R}_t$  and  $\mathbf{G}^{-1}(\cdot)$  is the gadget decomposition function which satisfies  $\mathbf{G}^{-1}(a) \cdot \mathbf{G} = a + e \pmod q$  for  $a \in \mathcal{R}_q^2$ , where  $e$  is some error introduced by the decomposition.

*CMUX gate.* With the given external product, we can build a small circuit called CMUX [8] which takes three inputs  $a, b$ , (RLWE ciphertexts) encrypting  $m_a, m_b$  respectively, and  $\mathbf{C}$  (an RGSW ciphertext encrypting a bit), and outputs either of  $a$  or  $b$  depending on the value which  $\mathbf{C}$  encrypts. The CMUX gate with the three inputs are defined as follows:  $\text{CMUX}(\mathbf{C}, a, b) = (b - a) \square \mathbf{C} + a =: c$ , where  $c$  encrypts  $m_b$  if  $\mathbf{C}$  is an encryption of 1, otherwise  $m_a$ .

*Conversion.* We refer to an efficient conversion algorithm (Algorithm 4 of [5]) to switch the format of a ciphertext from RLWE form to RGSW, while preserving the message  $m$ . In our case, the algorithm accepts  $\ell$  RLWE ciphertexts  $\{\text{RLWE}_s(m \cdot g^j)\}_{j \in [\ell]}$  as input and outputs  $\text{RGSW}_s(m)$ . To run this algorithm, an additional public evaluation key denoted by  $\text{ksk}$  is needed. This key is precomputed and sent by the client during the setup phase. We call the algorithm  $\text{RLWEtoRGSW}$  throughout the paper.

### 3.2 Homomorphic De-Multiplexer

The goal of the homomorphic de-multiplexer in our ORAM is to output a unit vector which contains 1 on a desired position. A similar functionality called homomorphic traversal is discussed in [10]. Given a binary tree of depth  $L$ , this algorithm moves a value from the root to a desired leaf. In ORAM, the client needs to indicate the desired item to be accessed without revealing its index to server. So we leverage this technique to distinguish the desired item from other database elements. Assuming that a server stores  $n$  data elements, we prepare a complete binary tree with level  $L = \log n$ . If the client wants to access the  $i$ -th element from the database, it can homomorphically index the  $i$ -th leaf with an encryption of 1, and the rest with encryptions of 0 via homomorphic de-multiplexing. Given these  $n$  leaves, the server can run the desired operation exclusively at the desired item because an operation on the  $i$ -th position can be only activated with an encryption of 1. Recall that the server cannot distinguish between encryptions of 0 or 1.

Unlike the approach of [10], the client only prepares  $\lceil \log n \rceil$  bits which represent a bit-decomposition of the index  $i$ , encrypts them all in RGSW format and transmits the resulting ciphertexts to server. The server runs the algorithm with  $\log n$  encrypted bits as controller bits, one for each level of the tree. In our case, all nodes on the same level of a tree use the same controller bit, whereas [10] requires different inputs for each decision node. At the end of the algorithm, we obtain an encryption of 1 on the  $i$ -th leaf from the left and encryption of 0 on all the other leaves.

We call this algorithm  $\text{HomDemux}$  and present it in Algorithm 1. In our instantiation,  $\text{HomDemux}$  takes  $\log n$  RGSW ciphertexts (the encrypted controller bits) and an integer for the root value, then outputs  $n$  RLWE ciphertexts (the leaves) which can be interpreted as an encrypted a unit vector of dimension  $n$ .

We note that the above algorithm outputs a vector of RLWE ciphertexts of dimension  $n$ , where the desired position has an encryption of  $r \geq 1$ . Technically, the output is not a unit vector if



---

**Algorithm 1** Homomorphic de-multiplexer HomDemux

---

```
1: Input:  $\log n$  controller elements  $\{c_0, \dots, c_{L-1}\}$ , and the root value  $r$  .
2: Output:  $n$  values of leaves:  $z_0, \dots, z_{n-1}$ 
3: Initialize root:  $b_0 \leftarrow r$ 
4: Initialize the node values:  $b_i := 0$  for  $i \in \{1, \dots, 2n - 2\}$ 
5: for  $i \leftarrow 0, \dots, L - 1$  do
6:   for  $j \leftarrow 0, \dots, 2^i - 1$  do
7:      $b_{2^{i+1}+2j-1} := b_{2^i-1+j} - b_{2^i-1+j} \cdot c_i$ 
8:      $b_{2^{i+1}+2j} := b_{2^i-1+j} \cdot c_i$ 
9: for  $i \leftarrow 0, \dots, n - 1$  do
10:   $z_i := b_{2^{L+1}-1+i}$ 
11: return  $z_0, \dots, z_{n-1}$ 
```

---

$r \neq 1$ , but eventually we obtain a unit vector of RGSW ciphertexts of dimension  $n$  in our ORAM instantiation, after running additional algorithm called RLWetoRGSW.

## 4 Core Design of Panacea

Here we present our core design for single query ORAM with  $O(1)$  bandwidth blowup and no client-side memory overhead. In Sections 5 and 6 we extend this design to improve server performance by allowing multiple queries to be sent in batches.

### 4.1 Design Description and Overview

We begin with a high-level description of how our algorithm works in the plaintext setting, then describe how it is lifted to the FHE setting.

1. The client sends  $(\mathbf{a}, \mathbf{op}, \mathbf{data})$ , where  $\mathbf{a}$  is the logical address of a requested block,  $\mathbf{op}$  represents either a read or write operation, and  $\mathbf{data}$  is the new data.
2. The server de-multiplexes  $\mathbf{a}$  into a unit vector  $(l_0, \dots, l_{n-1})$  where  $l_{\mathbf{a}} = 1$ , and the remaining values are 0, then responds with the result of the dot-product  $\langle (l_0, \dots, l_{n-1}), (d_0, \dots, d_{n-1}) \rangle$ .
3. To update, the server runs a simple circuit on every element  $d_i$  of the database:
  - Let  $\mathbf{temp}_i \leftarrow \mathbf{if} (\mathbf{op} = \text{Read}) d_i \mathbf{else} \mathbf{data}$ .
  - Update the database entry  $d_i \leftarrow \mathbf{temp}_i$ .

Now we give an overview of the same construction using FHE:

**Client: Query Generation** A query consists of a 3-tuple:  $(\mathbf{a}, \mathbf{op}, \mathbf{data})$ , following the same semantics as the plaintext version, except all the elements are encrypted.

The client chooses an index  $i \in [0, \dots, n - 1]$ , and computes its binary bit-decomposition to obtain  $\log n$  bits, denoted by  $\epsilon_0, \dots, \epsilon_{\log n - 1}$ . The client then encrypts these  $\log n$  bits to generate  $\mathbf{a}$ . Based on the desired operation  $\mathbf{op}$  (either Read or Write), the client generates an encryption of 0 or 1:  $\mathbf{op} = \text{Enc}(0)$  or  $\mathbf{op} = \text{Enc}(1)$  respectively. The final element in the query is  $\mathbf{data}$ , which is an encryption of zero in the case of a Read query or the actual data to be written in the case of a Write query.

**Server: Main computation** Once the server receives a query from the client, it executes the following two phases in succession:

1. **Response phase:** The server runs  $\text{HomDemux}(a, r)$ , the homomorphic de-multiplexer, on the input to generate an encrypted unit vector of dimension  $n$  indicating the desired position that the client wants to access, and the root value  $r$  which will be moved to the desired component of the output. Suppose  $r = 1$ , then the server computes a dot product between the unit vector and the data array to obtain the value at the requested position. Finally, the server sends the result to the client. Regardless of the operation, the client retrieves the original value at the desired location. If the  $\text{op}$  is **Read**, the client can access what it intended to retrieve (the  $i$ -th item). In case of a write operation, the client will ignore the received value. The actual database update (write) phase occurs after the response.

2. **Update Phase:** The Server creates a temporary array of  $n$  elements which contains either the original data elements or the updated value  $\text{data}$ , depending on  $\text{op}$  by running the function called **RW** which achieves the following: if  $\text{op}$  is **Read**, the temporary array copies all original data elements; and if  $\text{op}$  is **Write**, the client input  $\text{data}$  is copied to every  $n$  elements.

Then the server runs the **CMUX** gate with the  $n$  leaves each as a controller bit (which are the output of **HomDemux**) and as inputs the corresponding temporary element and the original data denoted as  $d_j$  for each  $j \in [0, n - 1]$ . In more detail, the  $n$  leaves contain only one encryption of 1 at the desired position (the  $i$ -th leaf) and the remaining elements are all encryptions of 0. Therefore, the  $i$ -th element will be updated with  $\text{data}$  if  $\text{op} = \text{Write}$ . Otherwise, it is updated with the original value  $d_i$ , meaning that the plaintext it encrypts remains the same eventually.

Every computation is done over encrypted elements, so that the server is oblivious to what operation is given and what block is updated or returned to the client.

## 4.2 Instantiation based on FHE

We describe our protocol using FHE ciphertexts as defined in Section 3. Let  $i$  be binarized as  $i = (\epsilon_0, \epsilon_1, \dots, \epsilon_{s-1})_2$ , where  $2^s = n$ . We show how data elements and the query elements are encoded in the following:

- $d_j$ : an RLWE sample under client's key  $K$ ,  $\forall j \in [0, \dots, n - 1]$
- $\mathbf{a} := (\text{RGSW}_K(\epsilon_0), \dots, \text{RGSW}_K(\epsilon_{s-1}))$
- $\text{op} := (\text{RGSW}_K(b_{\text{op}}))$ , if  $b_{\text{op}} = 0$ , it encodes **Read**. Otherwise, it encodes **Write**.
- $\text{data} := \text{RLWE}_K(\alpha)$ , where  $\alpha$  is an update value if  $\text{op} = \text{Write}$ , otherwise,  $\alpha$  is any random value.

After the server receives a query from a client, it runs  $\text{RW}(\text{op}, \text{data}, d_j)$  for each data element  $d_j$ . The algorithm is defined as follows:

- $\text{RW}(\mathbf{C}, a, b) \rightarrow c$ :
  - Given an input of an RGSW ciphertext  $\mathbf{C}$  and two RLWE ciphertexts  $a, b$  encrypting  $m_0, m_1$  respectively, it outputs an RLWE ciphertext  $c$  which encrypts either  $m_0$  or  $m_1$ .
  - Computes  $c := \text{CMUX}(\mathbf{C}, a, b)$

Hence, if  $\mathbf{C} = \text{RGSW}_K(0)$  (which is  $\text{op} = \text{Read}$ ), the output  $c$  is an RLWE ciphertext encrypting  $m_1$  (the original data). After each component of the output of **HomDemux** is converted to an RGSW ciphertext via  $\text{RLWEtoRGSW}$ <sup>5</sup>, the RGSW ciphertexts are used as controller bits of a **CMUX**

<sup>5</sup> We used the conversion algorithm: Algorithm 4 of [5].

gate to select either  $\mathbf{temp}_j$  or  $d_j$ . The final dot product step consists of performing  $n$  component-wise external products between  $n$  RGSW ciphertexts  $\{\mathbf{L}_j\}_{j \in [0, \dots, n-1]}$  and  $n$  RLWE ciphertexts  $\{d_j\}_{j \in [0, \dots, n-1]}$ . With the above definitions of encoding and functions, we describe the server side instantiation our ORAM protocol in Algorithm 2.

---

**Algorithm 2** ORAM protocol on server’s side

---

- 1: **Input:**  $(\mathbf{a}, \mathbf{op}, \mathbf{data})$ , where  $\mathbf{a}$  is the logical address of the requested block,  $\mathbf{op}$  is either Read or Write, and  $\mathbf{data}$  is the value written to the block at address  $\mathbf{a}$  if  $\mathbf{op} = \text{Write}$ . We note that everything in the query is encrypted under an FHE scheme.
  - 2: **Notation:**
    - $n$  := the number of data element.
    - $d_i$  := the  $i$ -th data element stored in a server.
    - $\mathcal{L} := \{l_0, \dots, l_{n-1}\}$ ; the set of value of leaves.
    - $\mathbf{temp}$  := temporary data element.
  - 3: Server sets  $y := 0$
  - 4: **for**  $i \leftarrow 0, \dots, \ell - 1$  **do**
  - 5:     Server runs  $\text{HomDemux}(\mathbf{a}, g^{i+1}) \rightarrow \mathcal{L}_i$
  - 6: **for**  $j \leftarrow 0, \dots, n - 1$  **do**
  - 7:     Server runs  $\text{RLWEtoRGSW}(\{l_{i,j}\}_{i \in [0, \dots, \ell-1]}, \text{ksk}) \rightarrow \mathbf{L}_j$
  - 8:     Server computes  $y := y + d_j \square \mathbf{L}_j$
  - 9: Server sends  $y$  to the client
  - 10: **for**  $j \leftarrow 0, \dots, n - 1$  **do**
  - 11:     Server runs  $\text{RW}(\mathbf{op}, d_j, \mathbf{data}) \rightarrow \mathbf{temp}$
  - 12:     Server computes  $d_j := \text{CMUX}(\mathbf{L}_j, d_j, \mathbf{temp})$
- 

### 4.3 Complexity Analysis

The communication complexity of the query is  $O(\log n)$  since the client sends only  $\log n$  encrypted bits. For every query, the server sends exactly one encrypted block to the client as response. Therefore, we also have an overall  $O(1)$  bandwidth blow-up as existing FHE-based ORAM designs [5,12]. Due to our stateless strategy, the server has to touch all database elements to guarantee security, hence the computation complexity is  $O(n)$ . In more detail, we run  $\ell \cdot n/2, n, \ell \cdot n, n$  and  $n$  external products for HomDemux, RW, RLWEtoRGSW, computing  $y$  and updating data, respectively. Since  $\ell$  is a parameter of the underlying FHE scheme, it is independent of  $n$ .

Since we separate the protocol into two phases: Response and Update, the server’s response latency from the client’s perspective would be equivalent to the running time of the response phase, which consumes  $(\ell/2 + \ell + 1) \cdot n$  external products. After responding, the server performs  $2n$  external products in the update phase. The server’s total time for each query is the sum of the duration of both phases.

### 4.4 Security

The security of our ORAM scheme stems directly from the semantic security (IND-CPA) of the underlying homomorphic encryption scheme<sup>6</sup>. Our queries consist of FHE ciphertexts, encoding the queried database index, desired operation, and potential update value. Semantic security ensures

---

<sup>6</sup> We instantiated our protocol with an (R)LWE based FHE scheme (which is IND-CPA secure).

that the server cannot learn any information about the underlying plaintexts of the query elements. The security of our design can be expressed through the following theorem.

**Theorem 1 (Security of  $\text{Panacea}_{\text{core}}$ ).** *Assuming IND-CPA security of the underlying FHE scheme  $\mathcal{E}$ , and assuming  $\mathcal{E}$  is correct except a failure probability negligible in a security parameter  $\lambda$ ,  $\text{Panacea}_{\text{core}}$  achieves security as defined in Definition 1 with the correctness parameter  $\mu$  negligible in  $\lambda$ .*

We refer to Appendix A for the proof of the above theorem. The theorem relies on the correctness and security of the underlying FHE scheme. However, when instantiating, we require an additional assumption of circular security which is always assumed in any FHE based protocol due to the use of key material (the key switching key in our case for RLWEtoRGSW) when encrypting key-dependent information. Since there is no known attack on circular security, we believe that it would be safe to rely on such an assumption without harm on our concrete security, as is the case in other similar works.

## 5 Multi-query ORAM with Amortized Computation Cost: Method 1

The design of ORAM presented in Section 4 handles one query at a time and incurs a server-side computational overhead of  $O(n)$  for each query. In this section, we present a method to reduce the (amortized) server-side computation cost for a batch of  $k$  queries on distinct elements over  $\tau$  processor threads. For simplicity, we assume the number of threads to be equal to the number of queries ( $\tau = k$ ). However, all the available processor threads can be fully utilized as long as  $\ell \cdot k \geq \tau$ . Our protocol is described in Algorithm 3 and Algorithm 4.

---

### Algorithm 3 Multi-query ORAM: Multi-Threaded Step

---

- 1: **Input:**  $\{(\mathbf{a}_i, \text{op}_i, \text{data}_i)\}, i \in [k]$ , where  $k$  is the number of queries and the rest are the same as Algorithm 2.
  - 2: **Notation:** we use the same notation as Algorithm 2.
  - 3: **for** every thread  $i \in [k]$  **do**
  - 4:     run  $\ell$  times of  $\text{HomDemux}(\mathbf{a}_i, g^s)$  for  $s \in \{1, \dots, \ell\}$  followed by RLWEtoRGSW to obtain  $\mathbf{L}_{i,j}$ .
  - 5:      $y_i \leftarrow 0$
  - 6:     **for**  $j \in [0, n-1]$  **do**
  - 7:          $y_i := y_i + d_j \boxplus \mathbf{L}_{i,j}$
  - 8:     The server sends  $\{y_i\}_{i \in [k]}$  to the client.
  - 9:     **for**  $j \in [0, n-1]$  **do**
  - 10:          $\text{temp}_{i,j} := \text{RW}(\text{op}_i, d_j, \text{data}_i) \boxplus \mathbf{L}_{i,j}$
  - 11:      $(\mathbf{L}_{i,j}, \text{temp}_{i,j})$  is kept for use in Algorithm 4.
- 

---

### Algorithm 4 Multi-query ORAM: Merge and Update Step

---

- 1: **let**  $\text{temp}_i := \{\text{temp}_{i,0}, \dots, \text{temp}_{i,n-1}\}, \mathbf{L}_i := \{\mathbf{L}_{i,0}, \dots, \mathbf{L}_{i,n-1}\}$
  - 2:  $\text{temp} := \sum_{i=1}^k \text{temp}_i, \bar{\mathbf{L}} := \sum_{i=1}^k \mathbf{L}_i$
  - 3:  $\text{CMUX}(\bar{\mathbf{L}}_j, \text{Enc}(d_j), \text{temp}_j), \forall j \in [0, \dots, n-1]$    ▷ Effectively, if  $\bar{\mathbf{L}}_j = \text{Enc}(1)$  it outputs  $\text{temp}_j$ ,  $\text{Enc}(d_j)$  otherwise.
- 

Algorithm 3 parallelizes Algorithm 2 except for Lines 8 and 12. Note that, only one entry with a distinct position is not an encryption of zero in each  $\text{temp}_i$ . Therefore, in Algorithm 4, adding

all  $\text{temp}_i$  values does not destroy the value of the entry due to  $k - 1$  zeros. As a result,  $\bar{\text{temp}}$  has  $k$  encryptions which encrypt non-zero values at the desired positions, with the rest being encryptions of zero. Moreover, the elements of  $\bar{\mathbf{L}}$  indicate the positions of the non-zero elements.

In essence, the first step (Algorithm 3) results in  $O(n)$  multiplications parallelized over each available thread, and the second step (Algorithm 4) merges the results by applying  $2n$  multiplications and  $k$  additions. Thus, the latency to process and respond to  $k$  queries is same as that of a single query, as  $O(n)$  operations are performed before responding to the client. Similarly, the response is sent to the client before performing the database update.

We make two observations where this method achieves performance gains when compared to running (a multithreaded version of) Algorithm 2 sequentially for  $k$  (distinct) queries. First, during the de-multiplexing step of Algorithm 2, if the number of threads available is greater than the number of decomposition levels  $\ell$ , then the additional threads would remain unused. In the method described in this section, all threads available would be utilized as long as  $\ell \cdot k \geq \tau$ . Second, instead of performing  $k \cdot n$  applications of the CMUX gate at the end, we sum the ciphertexts and only perform  $n$  CMUX operations.

## 6 Multi-query ORAM with Amortized Computation Cost: Method 2

In this method, we use an existing batching technique from the literature to achieve a sublinear server-side amortized computational cost when considering a batch of  $k$  queries. However, the proposed batching techniques come with their own trade-offs: the networking overhead when batching is much higher than the baseline. Additionally, batch codes require a redundancy of elements in the database, which significantly increases the server’s storage overhead. We provide an overview of batch codes and introduce our construction below.

*Batch Codes.* A batch code, parameterized by the 4-tuple  $(n, m, k, b)$ , takes as input a database with  $n$  elements, and outputs a set of  $m$  (possibly distinct) elements distributed among  $b$  buckets, such that any  $k$  elements from the original database can be retrieved by fetching at most one element from each of the  $b$  buckets. We want  $m < kn$  to have any performance improvement for the server.

*Probabilistic Batch Codes (PBC).* A probabilistic batch code, parameterized the 5-tuple  $(n, m, k, b, p)$ , is a relaxed version of batch codes which allows a failure probability of  $p$  to retrieve all  $k$  elements when the batch elements are chosen uniformly at random (without replacement). This introduces a probability  $p$  of encountering a batch of  $k$  elements such that there is no way to retrieve all the elements in that batch by fetching at most one element from each bucket. Ideally, we target minimizing the probability of failure as much as possible to maximize the probability of a successful execution of our protocol.

### 6.1 Improving Performance Using PBC

We use a PBC based on reverse cuckoo hashing. Our technique draws inspiration from the batching technique used in the PIR protocol: SealPIR [2]. One key difference between ORAM and PIR is that PIR protocols only provide read operations on the database, whereas ORAM schemes provide both read and write operations. Additionally, all data elements would be encrypted in the context of ORAM.

Using PBC, the database would be divided into  $b$  buckets using  $w$  pre-specified (not necessarily cryptographic) hash functions. First, the server allocates a total of  $m = w \cdot n$  elements into  $b$

buckets, such that there would exist  $w$  instances of each element spread across  $b$  buckets. Then, for each batch of  $k < b$  queries, the client accesses exactly one element from each bucket. We describe the details of this design and its underlying components below.

**Database Allocation by Server** Let  $h_1, \dots, h_w$  be  $w$  distinct hash functions. Since the client and the server need to agree on some hash functions, the hash functions are publicly specified as part of the protocol. Given a database of  $n$  elements, each element is hashed based on its index in the original database. The actual element is encrypted and remains encrypted throughout the process. Suppose an element at index  $\iota$  produces the following hash values:  $i_1 = h_1(\iota), \dots, i_w = h_w(\iota)$ . The server adds the elements from the buckets  $i_1, \dots, i_w$ . The process is then repeated for all distinct elements in the database. Upon completion, each element will have  $w$  instances spread over  $b$  buckets (possibly non-distinct). Depending on the hash functions, it is possible that there are multiple instances of the same element in a bucket, but only with small probability. However, the presence of two elements in one bucket does not impact the security of ORAM and only influences the failure probability of PBC. We further discuss more this failure probability and its implication in Section 6.4.

**Batch-query by Client** For every batch of  $k$  (read/write) queries, the client is expected to perform  $b$  accesses, one from each of the  $b$  buckets. For each access per bucket, the client can run the core protocol described in Section 4. The client selects the elements for those  $b$  accesses in a way that satisfies all the  $k$  desired read/write operations. To that end, the client uses the *reverse cuckoo hashing* technique with the  $w$  hash functions as described below.

The problem can be looked at as a balls-and-bins problem. The client has to place  $k$  balls (the intended read/write operations) into  $b$  bins (the buckets in the database), where each bin can have at most one ball. For a ball (the index of an element)  $\iota$  the client computes  $w$  candidate buckets by applying the hash functions. Then places the ball in one of the empty candidate bins. If none of the candidate bins are empty, the client picks one uniformly at random, removes the existing ball  $\iota_{old}$  from the chosen bin, and places the new ball  $\iota$  there. For the removed ball  $\iota_{old}$ , the client runs the insertion procedure again, and if that causes another ball to be removed, this procedure goes on recursively for a maximum number of iterations.

If the client can successfully place all the  $k$  balls into  $b$  bins, that becomes the assignment for elements in each bucket the client should access from the server. There is also a small chance of failure to place all the  $k$  balls into  $b$  bins, we evaluate the failure probability in Section 6.4. Since the client and the server are using the same hash functions, if assignment puts an element  $\iota$  in bin  $i$  for the client, that element will be available in bucket  $i$  on the server database. Now, the client can run one instance of the core ORAM protocol described in Section 4 for each bucket. Note that, for  $(b - k)$  buckets, which were empty after placing  $k$  balls into  $b$  bins, the client generates dummy read requests. Since the client accesses one element from each bucket, and no bucket is touched more than once in one batch, the server does not know which buckets correspond to which of the  $k$  accesses requested by the client. However, to access a specific element in a bucket, the client needs to know the index  $j$  of the element in that bucket for the index  $\iota$  in the original database. Moreover, since the elements in the database are encrypted and each element has exactly  $w$  redundant copies, the other  $(w - 1)$  copies need to be updated as well for each write access. Otherwise, the database would lose consistency, and any future queries might not return correct (up-to-date) results. We describe below how we solve the above two problems.

---

**Algorithm 5** ORAM protocol using PBC

---

1:  $\{D_i\}_{i \in [b]}$  := the database divided into  $b$  buckets, initially all buckets are empty.  
2:  $d_\iota$  := the element at index  $\iota$  in the original database  $DB$ .  
3:  $\{h_t\}_{t \in [w]}$  := the hash functions used for PBC.  
4:  $I$  := **IndexMap**: the mapping between an original database index  $\iota$  and the pairs  $(i, j)$  denoting bucket index and the location inside the bucket.

5: **function** SERVER:SETUP(Database  $DB$ )  
6:   **for**  $i \leftarrow 0, \dots, b - 1$  **do**  
7:      $\text{counter}_i := 0$   
8:   **for** each index  $\iota$  in  $DB$  **do**  
9:     **for**  $t \leftarrow 0, \dots, w$  **do**  
10:        $i := h_t(\iota)$ ; Append to  $D_i$  the element  $d_\iota$   
11:       Add the 3-tuple  $(\iota, i, \text{counter}_i)$  to  $I$   
12:        $\text{counter}_i := \text{counter}_i + 1$

13: **function** CLIENT: BATCHQUERY( $\{(a_t, \text{op}_t, \text{data}_t)\}_{t \in [k]}$ )  
14:    $\{(i_t, j_t, \text{op}'_t)\}_{t \in [k]} \leftarrow \text{BatchEncode}(I, \{(a_t, \text{op}_t)\}_{t \in [k]})$   
15:   **for**  $t \leftarrow 0, \dots, k - 1$  **do**  
16:     Send request on  $D_{i_t}$  for each input  $(j_t, \text{op}'_t, \text{data}_t)$

17: **function** SERVER: BATCHRESPONSE( $\{(j_i, \text{op}_i, \text{data}_i)\}_{i \in [b]}$ ) ▷  $(j_i, \text{op}_i, \text{data}_i)$  are encrypted for Server.  
18:   **for**  $i \leftarrow 0, \dots, b - 1$  **do**  
19:     Run Algorithm 2 on  $D_i$  on input  $\{(j_i, \text{op}_i, \text{data}_i)\}$  ▷ The response  $y_i$  is sent back during the process.  
20:     ConsistencyCorrection() ▷ See Algorithm 6.

21:   ConsistencyCorrection()

22: **function** CLIENT: EXTRACT( $\{(a_t, \text{op}_t)\}_{t \in [k]}, \{y_1, \dots, y_b\}$ )  
23:    $x_1, \dots, x_b := \text{Decrypt} \{y_1, \dots, y_b\}$   
24:   **return** BatchDecode( $I, \{(a_t, \text{op}_t)\}_{t \in [k]}, \{x_1, \dots, x_b\}$ )

---

## 6.2 Mapping Indices

In order to access an element from a bucket the client needs to know the index  $j$  of the element in the bucket for its original index  $\iota$  in the database. We solve that problem using an `IndexMap` which stores this mapping. The client can store the `IndexMap` throughout the time it uses the database which that adds a small memory overhead, in order to save query generation time. For a database with one million entries, the total size of `IndexMap` is less than 9 MB for our chosen parameters.

It is to be noted that the indices of the elements are used as inputs to the hash functions during the process of allocating them to the buckets. Therefore, once the buckets are allocated by the server, `IndexMap` is never modified. Other ORAM designs that rely on client storage require the client to maintain some metadata representing the state of the database, and that needs to be updated after every read/write access and requires secure storage to protect privacy. On the contrary, `IndexMap` in our case can be public and does not require any updates. Moreover, if the server uses a pre-defined source of randomness (which does not break the security of the ORAM protocol), `IndexMap` becomes deterministic and can be provided to the client as part of the setup. In that sense, our client remains stateless: even if the client goes offline, it can easily retrieve/reconstruct the `IndexMap` from setup information.

We denote the method of producing  $b$  pairs of bucket indices and the corresponding indices in the buckets from  $k$  indices from the original database as `BatchEncode()`. This operation accepts as input  $k$  tuples  $\{(\iota_1, \text{op}_1), \dots, (\iota_k, \text{op}_k)\}$  and outputs  $b$  3-tuples  $\{(i_1, j_1, \text{op}_1), \dots, (i_b, j_b, \text{op}_1)\}$ . When the client receives the server’s response, it just needs to discard the  $(b - k)$  responses corresponding to the dummy requests mentioned above. We call this method `BatchDecode()`. We describe the ORAM algorithm using PBC in Algorithm 5.

## 6.3 Consistency Correction

Since our batching technique requires redundancy, all  $w$  copies of data elements need to be updated for each write access. With the above method alone<sup>7</sup>, only one of  $w$  copies would be updated, leaving the remaining copies as encryptions of the old data. Therefore, we introduce a new technique which also updates the remaining redundant  $w - 1$  blocks to avoid data inconsistency.

We explain our technique to correctly update all the copies with  $w = 3$  for simplicity, our instantiation also uses  $w = 3$  which we motivate in Section 6.4. This method can be extended to any  $w > 1$ .

We note that this correction is run after the merge and update phase (Algorithm 4) is executed on each bucket. Suppose that the three hash functions ( $w = 3$ ) are applied to index  $\iota$  and the resulting indices are given by  $(i_1, j_1)$ ,  $(i_2, j_2)$  and  $(i_3, j_3)$ , where  $i_*$  and  $j_*$  represent the bucket index and the position of an element inside the bucket respectively. After processing a batch, the server obtains the following for each pair  $(i, j)$  as a result of applying the homomorphic de-multiplexer (Section 3.2) on each bucket:

$\mathbf{L}_{i,j}$ : an RGSW ciphertext that encrypts 1 if the  $j$ -th element in the  $i$ -th bucket is accessed, or 0 otherwise.

$B_i$ : an RGSW ciphertext that encrypts 1 if the operation in the  $i$ -th bucket is a write operation, or 0 otherwise. This is the same as `op` from the client’s query (Section 4.2).

We present the method in Algorithm 6. And below the algorithm, we give an example to make readers understand how it works easily. First, we list up the following properties of our protocol.

---

<sup>7</sup> PBC without consistency correction



1. Client queries at most one element in each bucket. And all information contained in his query is encrypted.
2. Each batch query consists of the addresses of  $k$  distinct data elements.
3. Therefore, there are  $\omega$  corresponding  $\mathbf{L}_{i,j}$  bits which indicate the same fixed data element, and at most one of them is an encryption of 1.
4. Server knows which  $\omega$  positions contain the same data element due to the public index map, but still being oblivious to which item it is.

---

**Algorithm 6** ConsistencyCorrection after every batch

---

**1: Notation:**

- $V_{i,j} :=$  the encrypted value on the position:  $j$ -th element in the  $i$ -th bucket.
- $\{h_t\}_{t \in \{1,2,3\}} :=$  the hash functions used for PBC.
- $I := \text{IndexMap}$ : stores the mapping between an original database index  $\iota$  and the pairs  $(i, j)$  denoting bucket index and the location in the bucket.
- $\{\mathbf{L}_{i,j}\}$ ; the set of leaf values after running HomDemux on bucket  $i$ .

**2: for**  $\iota \leftarrow 0, \dots, n-1$  **do**
**3:**  $(i_1, j_1), (i_2, j_2), (i_3, j_3) :=$  query  $I$  for  $\iota$ .

**4:** **for**  $t \leftarrow 1, 2, 3$  **do**
**5:**  $B_{i_t} \leftarrow \text{op}_{i_t}$ 
**6:**  $v := V_{i_1, j_1} \boxtimes (1 - \mathbf{L}_{i_1, j_1} \boxtimes B_{i_1} - \mathbf{L}_{i_2, j_2} \boxtimes B_{i_2} - \mathbf{L}_{i_3, j_3} \boxtimes B_{i_3}) + (V_{i_1, j_1} \boxtimes \mathbf{L}_{i_1, j_1} \boxtimes B_{i_1} + V_{i_2, j_2} \boxtimes \mathbf{L}_{i_2, j_2} \boxtimes B_{i_2} + V_{i_3, j_3} \boxtimes \mathbf{L}_{i_3, j_3} \boxtimes B_{i_3})$ 
**7:**  $D_{i_1}[j_1] := D_{i_2}[j_2] := D_{i_3}[j_3] := v$ 


---

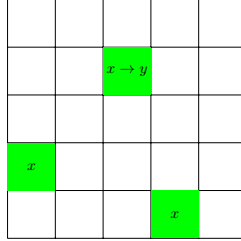


Fig. 1: An example of consistency correction of database contained in 5 buckets copied  $\omega = 3$  times.

Let's consider an example with the database structured like Figure 1. Each data element is copied  $\omega = 3$  times and distributed in 5 buckets (each row corresponds to each bucket in the figure). And an element  $x$  is stored in  $(2,3)$ ,  $(4,1)$ , and  $(5,4)$  positions. Since all elements are encrypted, the server only sees the random looking values, denoted by  $V_{2,3}$ ,  $V_{4,1}$  and  $V_{5,4}$  on the three positions. After server's update with a client's query, the element  $x$  on the position  $(2,3)$  is updated to  $y$ , meaning that the operation corresponding to the second bucket  $\text{op}_2 := B_2$  was WRITE (an encryption of 1), and the indicator bit for this position  $\mathbf{L}_{2,3}$  is an encryption of 1, and the rest  $\mathbf{L}_{4,1}$  and  $\mathbf{L}_{5,4}$  must be encryptions of 0. Until this stage,  $V_{2,3} = \text{Enc}(y)$ , and  $V_{4,1} = V_{5,4} = \text{Enc}(x)$  (note that the encryption algorithm is probabilistic, therefore the value of the two are different on the server's view).

Then server computes new value, denoted by  $V^{new}$ , for the 3 positions corresponding to the original element  $x$  like the following:

$$\begin{aligned}
V^{new} &= V_{2,3} \boxplus (1 - \mathbf{L}_{2,3} \boxplus B_2 - \mathbf{L}_{4,1} \boxplus B_4 - \mathbf{L}_{5,4} \boxplus B_5) \\
&+ (V_{2,3} \boxplus \mathbf{L}_{2,3} \boxplus B_2 + V_{4,1} \boxplus \mathbf{L}_{4,1} \boxplus B_4 + V_{5,4} \boxplus \mathbf{L}_{5,4} \boxplus B_5)
\end{aligned}$$

By the above third property, The terms multiplied by  $\mathbf{L}_{4,1}$  and  $\mathbf{L}_{5,4}$  become all 0. In other words,  $V^{new} := V_{2,3} \boxplus (1 - \mathbf{L}_{2,3} \boxplus B_2) + V_{2,3} \boxplus \mathbf{L}_{2,3} \boxplus B_2$ . Since  $\mathbf{L}_{2,3}$  and  $B_2$  are both encryptions of 1,  $V^{new}$  is an encryption of  $y$  which is the value on the position of (2,3) because  $V_{2,3} := \text{Enc}(y)$ . Again, any computation over ciphertexts results in a random looking value. Therefore, the final value  $V^{new}$  is not the same as the original  $V_{2,3}$ , even though both are encrypting the same element  $y$ .

Finally, the server copies  $V^{new}$  to the corresponding positions (2, 3), (4, 1), and (5, 4), meaning that both  $V_{4,1}$  and  $V_{5,4}$  are also changed to  $\text{Enc}(y)$ , while server still does not learn anything about  $y$ .

**Complexity** We note that consistency correction is run after server’s update as you can see in Algorithm 5. Since the server has to touch all  $n$  elements to guarantee the security of a stateless protocol, consistency correction should be done for all elements. The dominant operation in Algorithm 6 is the external product. Per  $\iota$ , it requires  $4 \cdot \omega$  external products. Therefore, the complexity is  $O(\omega \cdot n)$ . In total, the overall complexity of the whole protocol with PBC, still remains linear in  $n$ , in detail  $O(\omega \cdot n)$  since  $\omega$  is independent of  $n$  and it is chosen 3 in our protocol. We also stress that Algorithm 6 has to be executed before the next query batch is processed to guarantee correctness.

## 6.4 Failure Probability and Parameter Choices

There is a very small probability that the assignment of  $k$  balls in  $b$  bins will fail. However, that will only result in a failure to retrieve some  $k$  elements from a batch of queries. And that small probability directly translates to the correctness parameter  $\mu$ , and does not impact the privacy of the protocol. Below we provide an informal explanation about the failure probability, and refer to Appendix A.3 for a formal security theorem that reduces the failure probability of cuckoo hashing to the security of our ORAM protocol with PBC.

Analyzing the exact probability of failure, and determining the constant factors of cuckoo hashing still remains an open problem. Although there exist some works [13,15] that provide asymptotic estimates of the failure probability of cuckoo hashing, the hidden constants make it difficult to precisely determine the accuracy of the technique. Instead, we use empirical estimates of the failure probability as used in many other prominent works [6,2,3,33] that use cuckoo hashing. Chen et al. [6] estimate that the failure probability for different parameter choices; they show for  $w = 3$  and  $k > 200$ , the failure probability is  $\approx 2^{-40}$  with  $b = 1.5k$ . They additionally estimate that the failure probability is significantly high with  $w = 2$ , and does not improve much with  $w = 4$  over  $w = 3$ . Following their analysis, we choose  $k = 256$ ,  $w = 3$ , and  $b = 384$ . With that, the database has an additional 3x storage overhead, and the client has an additional 1.5x bandwidth overhead. However, since the access in each bucket is independent of other buckets for a single batch, then the server can run multiple accesses targeting different buckets in parallel.

It is important to note that, the client will know that the batch will fail and the exact elements that will not be retrieved, before even sending the batch query to the server. In such cases, for all practical purposes, the client can retrieve the failed elements with an additional batch-query. Therefore, the protocol execution is not disrupted because of such (highly unlikely) failures.

## 6.5 Tradeoffs And Comparison With Method 1

With our batching technique, we reduce the server-side computational cost of by several factors (as demonstrated in our experiments in Section 7). However, this improvement comes at a bandwidth cost of 1.5x when compared to our Method 1 or the core protocol and a storage cost as the database takes 3x more space. Additionally, there is a slight increase in client-side memory overhead compared to Method 1 due to the storage of the hash table (see Table 1). Since each component of `IndexMap` consists of a few bits (bit length of an index), the actual overhead does not have a big impact on the client’s performance. On the other hand, if running cuckoo hashing is fast enough, then the client does not need to store `IndexMap`, instead, he generates the hash every time he queries. Then the memory complexity on the client side becomes  $O(1)$ , but the query generation complexity will increase to  $O(n)$  (running hash functions over  $n$  elements), which is a fair trade-off.

In Method 1, we mainly optimize the number of read/write operations to the database: the overall computation cost for the server is still  $O(n)$ . If disk-IO per block is expensive (e.g., very large block size) or the cost of computation is not a concern (availability of a powerful cluster), Method 1 could be beneficial to optimize the bandwidth. However, given that server-side computational overhead is much higher than disk access, Method 2 would be more useful to optimize the server computation time.

## 7 Implementation and Evaluation

Our protocol leverages the TFHE scheme [8] which supports every homomorphic operation we use. We provide an implementation in the Rust Programming Language<sup>8</sup> using the Concrete Core library<sup>9</sup> [9] for homomorphic operations. The source code is available on GitHub.<sup>10</sup> We include the dependency manifest (`Cargo.lock`) and the parameter sets used in our experiments (`params.json`) to ensure reproducible results.

### 7.1 Experimental Setup

To simulate a Server implementing our scheme, we benchmarked our implementation on a dedicated cloud instance running Red Hat Linux. The instance was equipped with an Intel<sup>®</sup> Xeon<sup>™</sup> Platinum 8360Y CPU (36-core@2.4ghz) and 2TB of RAM.

To simulate a client, we compiled our code, targeting a Linux PC equipped with an Intel<sup>®</sup> Core<sup>™</sup> i5-6600 CPU (4-core@3.3ghz) and 8GB of RAM, as well as a 2020 Apple MacBook Pro with an M1 chip and 8GB of RAM. In contrast with our server setup, benchmarks evaluated on both client setups were limited to a single-thread for ease of comparison.

We assume that the client and the server agree on the database and FHE parameters prior to execution. Additionally, during setup, the client generates their keys and sends the evaluation keys to the server. The server sets up a dummy database (or a database consisting of trivial RLWE encryptions of zeros). We benchmark successive simulations of our protocol for a variable database size progressing from  $n = 2^{12}$  to  $n = 2^{19}$  using the same hardware. Our instantiations use parameters in Table 3, yielding 119 bits of security [1] (we set the same parameter sets  $(N, q, \sigma)$  as Onion Ring Oram).

<sup>8</sup> Toolchain: Rust version 1.68.0 nightly-x86\_64-unknown-linux-gnu

<sup>9</sup> “concrete-core” version: 1.0.2

<sup>10</sup> <https://github.com/KULeuven-COSIC/Panacea>

Table 3: TFHE Parameters

Parameter	Value
standard deviation	$2^{-55}$
polynomial degree $N$	2048
decomposition parameters for key switching $(g, \ell)$	$(2^5, 11)$
decomposition parameters for query $(g, \ell)$	$(2^5, 9)$
plaintext modulus $t$	$2^8$
ciphertext modulus $q$	$2^{64}$

## 7.2 Bandwidth

Table 4: Bandwidth blowup (BB) and the actual bandwidth cost for 384KB data element size when  $n = 2^{19}$ . We used method 2 (PBC) for our amortized scenario.

	ORAM type	bandwidth BB		amortized BB	
Stateful	Path ORAM	28.5 MB	76	57 MB	152
	OnionRing ORAM	2 MB	5.33	246MB	640
	OnionRing ORAM (with query packing)	2 MB	5.33	4.8 MB	12.8
Stateless	Panacea	9 MB	24	10.5MB	28
	Panacea (with query packing)	3 MB	8	3 MB	8

So far, we have shown that FHE grants us optimal communication overhead for stateless ORAM, as first achieved with stateful ORAM by [12]. Theoretically, our construction does not impose restrictions on the choice of parameters, which is why we achieve  $O(1)$  bandwidth blowup. In other words, the ciphertext size can be minimized as long as it can encrypt the message bits, independently of  $n$ . In our implementation, we set  $q = O(\log n)$  to show the best performance in a way that is comparable with current FHE based instantiations, including Onion Ring ORAM. Our main algorithm, and that of Onion Ring ORAM have a multiplicative depth of  $O(\log n)$ , implying  $q = O(\log n)$  as ciphertext size. As a result, the bandwidth complexity in both implementation becomes  $O(\log n \cdot \log q) = O(\log n \cdot \log \log n)$ . However, both designs easily achieve  $O(1)$  actual bandwidth blow-up, by compromising computational efficiency through requiring bootstrapping.

The goal of both our design and those of previous approaches is divergent as they both target different use cases. We try to level the playing ground for comparison as much as possible by demonstrating practicality of stateless ORAM with our optimizations in this section. We also attempt to record actual bandwidth and computation times, compared to previous designs under similar conditions.

Unlike previous stateful designs, our query cannot contain any plaintext to guarantee the security. Therefore, the actual communication cost for queries would be worse than that of many stateful designs due to size of FHE ciphertexts.

Fortunately, since the client sends fresh ciphertexts, the encryption randomness component can be represented as a seed for pseudorandom function (PRF) [32,8], and then expanded into a polynomial. This technique is applicable to RLWE and RGSW ciphertexts, and we can use it to reduce our bandwidth cost by a half. Note that this is not possible for the response ciphertexts since these are not fresh anymore.

With our concrete implementation parameters, one fresh RGSW ciphertext costs 288KB and one fresh RLWE ciphertext costs 16KB (encrypting 2KB of message) as one response costs 16KB (we use the same technique of OnionRing ORAM [5] to reduce the size of response by reducing modulus from 64 bits to 32 bits). We require  $\log n$  RGSW ciphertexts to encode the chosen index  $a$  and one more for the operation  $op$ . We can consider a scenario similar to that of Onion Ring ORAM where their database is encoded with AES encryption which would be converted into RLWE ciphertexts during eviction, such that the size of **data** can be negligible, compared to other query elements. However, we stress this involves significant performance impacting costs in order to reduce bandwidth costs and such techniques are not necessary to achieve ORAM.

For a fair comparison of bandwidth, we also consider this setting: when  $n = 2^{19}$ , the query size consists of 20 RGSW ciphertexts ( $20 \times 288\text{KB} = 5.63\text{MB}$ ), and 384KB for AES encrypted **data**, resulting in 6MB. Then the server’s answer consists of 192 RLWE ciphertexts (to retrieve a data element of size 2KB) each of size 16KB, resulting in 3MB. The total communication cost is then 9MB. Due to the choice of parameters in Onion Ring ORAM [5]  $t = 2^{12}$ , it was possible that more data could be loaded (up to 3KB) in one ciphertext, resulting in a reduced server response size of 2MB. It is possible for us to set the same  $t$  in theory, but for large  $n = 2^{19}$ , we had to reduce the parameter to guarantee the correctness in our *actual implementation*.

Each bucket contains  $2^{12}$  elements (since  $b=384$ ), each query consists of 13 RGSW ciphertexts (3.66MB) and **data** of size 384KB, the answer is as same as the single query case (3MB). However, since we have 1.5x blowup from PBC, it results in 10.5MB ( $= 1.5 \times 7\text{MB}$ ).

If larger batches are needed, we can reduce amortized bandwidth more and gain computation time per bucket. For example, if we set  $b=1536$ , each bucket contains  $2^{10}$  elements, then the resulting amortized bandwidth will become 9.7MB; smaller than the single query case.

Onion Ring ORAM can show less bandwidth overhead than us, since their benchmarked queries are not encrypted using homomorphic encryption. On the other hand, their bandwidth increases in amortized scenario, due to huge amount of additional encrypted ingredients that would be transmitted during eviction. To reduce the high overhead, a query packing method is used to pack all the query bits in  $\ell$  RLWE ciphertexts, instead of sending  $\log n+1$  RGSW ciphertexts as we currently do. Even without this optimization, we can confirm providing much less bandwidth overhead than PathORAM due to our constant bandwidth blowup.

*Query Packing.* We can also use the same optimization technique of Onion Ring ORAM called query packing method to reduce the query size. Then, the server would have to unpack queries upon reception and convert them into the right format for processing. We call this conversion operation query unpacking. Then, there would be an additional server-side computational overhead of complexity  $O(\log n)$ . Query unpacking can be trivially parallelized, therefore it does not cause a significant impact to the total computation time. When we pack the client’s query (i.e. indices of the item, operation encoding) into  $\ell$  RLWE ciphertexts, the bandwidth consumption would be dominated by the server’s response: 3MB in this case. The result is given in the last row of Table 4.

We have also implemented our design with query packing by using a tweaked version of Algorithm 4 of [5] for  $n = 2^{19}$  without modifying our parameters. We note that the unpacking method (Algorithm 4 of [5]) causes the presence of a lot of additional noise, given the same parameters. Therefore, to guarantee correctness, we use a tweaked version of their algorithm (discussed in Appendix B). In our implementation, the unpacking algorithm consumed 69ms per RLWE ciphertext, hence the additional cost is around 13 seconds to unpack 20 RGSW ciphertexts for  $n = 2^{19}$ .

We note that our bandwidth blowup is only affected by the ciphertext expansion factor (ratio between ciphertext and plaintext sizes) of the underlying FHE scheme: Panacea maintains a constant bandwidth blowup regardless of the block size. On the other hand, Onion Ring ORAM [5] has another factor  $Z$  (the number of real blocks in each node/bucket of their tree structure) which depends on  $n$ . In order to keep the bandwidth blowup constant in practice, Onion Ring ORAM would require large block size in combination with query packing.

### 7.3 Computational Overhead

To demonstrate the practicality of our design we evaluate the computational overhead for the server.

**Single query and Method 1** For single query performance, with  $n = 2^{12}$ , the response time is 1.77s and the update duration is 0.81s. We used  $k = 36$  threads when implementing the single query protocol to benchmark the performance. Afterwards, we used Method 1 to handle  $k$  queries in one go using the same setup. As expected, Method 1 for  $k$  queries is faster than running single query (Algorithm 2) protocol  $k$  times on the same number of cores. This is due to the inability to parallelize all parts of the computation in the single query case as we observed in Section 5. Specifically, to process  $k$  queries, Section 5 consumes 28% less time on average to respond to the client when compared to Algorithm 2.

**Batching with PBC** When the protocol uses PBC, the client batches 256 queries and submits the whole batch to the server which processes it at once. In our experiments, we use a total of 36 threads (one thread per core) to parallelize server-side computations. Numbers in Table 5 show the averages taken over 5 independent runs of the experiment. The sum of the response duration and update duration represents the total time spent by the server to treat a query. The response duration specifies the elapsed duration between the server receiving the client’s query and transmitting the response. The update duration is equivalent to the time spent by the server to update the database after responding to the client. Figure 2 displays the linear growth of the amortized duration of server computation as the number of database elements increases.

We find a clear performance advantage when comparing with the single query mode. Using a database size of  $2^{12}$ , the server is over 180 times faster in terms of access duration.

Table 5: Computation time required by the server for database size  $n$ , with  $n$  from  $2^{12}$  to  $2^{19}$ , for the size of the batch  $k = 256$  with PBC. Numbers in brackets are amortized cost. All times are in seconds.

$n$	Response Duration	Update Duration	Total Time
$2^{12}$	2.47 (0.0096)	1.01 (0.0004)	3.48 (0.014)
$2^{14}$	9.53 (0.037)	2.89 (0.011)	12.42 (0.049)
$2^{16}$	38.08 (0.15)	11.04 (0.043)	49.13 (0.19)
$2^{18}$	147.92 (0.58)	48.02 (0.19)	195.94 (0.77)
$2^{19}$	296.43 (1.16)	94.83 (0.37)	391.26 (1.53)

We came across some difficulties when comparing our numbers directly with those of Onion Ring ORAM [5] since their implementation is not publicly available. Moreover, we conjecture that

the numbers presented in Onion Ring ORAM are theoretical projections which do not account for bottlenecks from data transfer speeds between CPU and RAM which we noticed during our experiments when using large database sizes. Memory bandwidth is a well-known bottleneck for FHE computation [36,17]. Therefore, we provide an analytical comparison below.

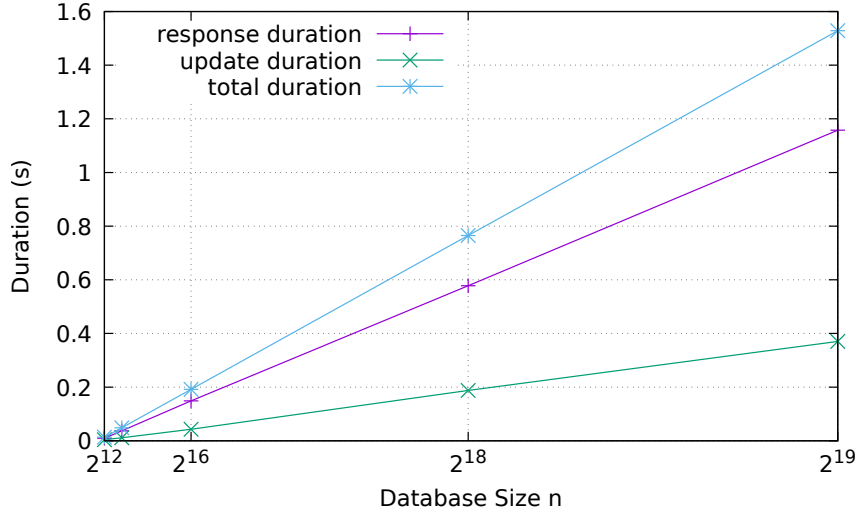


Fig. 2: Amortized duration of server computation with database size  $n$  from  $2^{12}$  to  $2^{19}$  and batch size  $k = 256$ . The  $x$ -axis denotes the database size  $n$ , and the  $y$ -axis denotes the duration (in seconds).

**Explanation and Analytical Comparison** We remind that our aim is not to beat the previous stateful designs, but rather to show that optimized stateless designs also can perform comparably to stateful protocols in practice. The main computation is performed over  $n$  data elements to guarantee the security, either sequentially or in parallel depending on the server’s resources and deployment scenario. Therefore,  $O(n)$  is an inevitable complexity. In fact, the response phase which mainly impacts on the latency consisting of  $(\ell/2 + \ell + 1) \cdot n$  external product in practice, where  $\ell$  is a parameter of the underlying FHE scheme. In our experiments, we set  $\ell = 9$ . Hence, at least  $14.5 \cdot n$  external products are performed. If we use Method 2, this number is multiplied by  $w = 3$  to handle  $k \geq 200$  queries at a time.

When comparing with an interactive and stateful design (mainly Onion Ring ORAM), we note that their construction has a default complexity of  $O(\log n)$  for both online and offline phases. The main operation during the online phase is an addition of  $\log n$  ciphertexts, which is extremely cheap when compared to other homomorphic operations. However, to commit writes on the remote database, an eviction protocol is required for every  $A$  accesses, during which the server runs an expensive algorithm  $\log n$  times interactively with the client. This algorithm is instantiated with FHE and some concrete parameters in [5]. However, we note that there exists a hidden factor of  $Z \log Z$  in their complexity analysis of eviction. This factor is a result of reshuffling  $Z$  blocks in each node (bucket) on a selected path during eviction. Precisely, the dominant complexity during the eviction comes from performing  $Z \cdot \log Z \cdot \log n \approx 2^{17}$  external products, where  $Z \approx 2^9$  according to their choice of parameters, when  $n = 2^{22}$ . Therefore, the dominant factor is not only limited by

$\log n$  anymore, but also by the number of slots ( $Z$ ) in every bucket is the key factor which impacts real performance. As a result,  $Z$  should also be chosen carefully according to  $n$ .

If we set  $k = A$ , we can compare the two different designs in the amortized scenario with  $k$  queries and obtain close results. The actual latency of their eviction phase also depends on how fast the client is at answering since it requires multiple client-server interactions. Additionally, our protocol parallelizes much better given additional server resources, whereas their eviction should be run sequentially and interactively, which also contributes positively to our practical performance. These factors should also be taken into account when applying such protocols in the real world.

**Client Performance: Method 2** One of the benefits of our stateless design is that the client has much less of a computational burden compared to stateful constructions. The client-side computation only consists of generating queries (encrypting indices) and decrypting responses from the server. The duration of performing one RGSW Encryption during setup is 0.17s for Intel i5-6600, and 0.065s for Apple M1. As such, the computation cost is small enough for the client to run efficiently even when using a normal computer.

On the other hand, Onion Ring ORAM necessarily requests the client to join the offline (eviction) phase after every  $A$  accesses. In the eviction phase, a client has to generate a permutation to reshuffle blocks in  $\log n$  buckets on a chosen path, resulting in having to perform  $O(\log n \cdot Z \cdot \log Z)$  encryptions. Moreover, the client also has to download  $Z$  data elements (which are encrypted) multiple times during the eviction phase.

## 7.4 Memory Usage

Our server’s memory overhead, is independent of the structure of the database: it always remains constant overhead, apart from Method 2 which relies on the number of hash functions that we use. On the other hand, tree-based stateful designs rely heavily on the tree depth ( $L$ ) and the number of slots ( $Z$ ) in each node to guarantee security. For Onion Ring ORAM, both parameters are tightly coupled with  $n$ . However, with the concrete parameters used for their implementation,  $Z$  and  $L$  were carefully chosen for  $Z \cdot 2^L$  to be bounded by  $4n$  to optimize results. Therefore, with our choice of  $w = 3$  in Method 2, we store  $3n$  elements with the server, and our storage overhead remains similar to Onion Ring ORAM’s in practice.

Regarding real-time server-side memory consumption, we recall from Section 6 the need to temporarily store  $w \cdot n$  RGSW ciphertexts  $\mathbf{L}_{i,j}$  in memory to perform the consistency correction algorithm. This introduces considerable memory usage since one RGSW ciphertext consists of  $2\ell$  RLWE ciphertexts. But it is possible to reduce the memory usage by a half if the consistency correction is performed as soon as possible, i.e., by performing consistency correction on the three entries in the encoded database that are mapped from the same original index right after they are available, instead of waiting for *Panacea<sub>core</sub>* to be completed on every bucket. We leave this optimization for future work.

## 7.5 Noise Growth

Due to the nature of FHE schemes, after performing a certain number of operations, ciphertexts accumulate noise over time. When the noise becomes too high, it would no longer be possible to decrypt ciphertexts successfully. This applies to our ORAM protocol: after a certain number of



(sequential) accesses, the result returned by the server may respond with ciphertexts that cannot be decrypted by the client anymore.

We show that our protocol can support over 100,000 (amortized) queries using Method 2 before bootstrapping is needed to refresh the noise budget. It is because the noise contained in the data is additively accumulated per access due to the homomorphic operation that we use called external product in [8].

The multiplicative depth of the protocol grows linearly in the number of sequential accesses. In every access, the new noise term to be added is generated via a series of external products (HomDemux and RLWEtoRGSW) among ciphertexts which have low noise. Let’s denote this term by  $v_q$  which does not depend on the noise contained in data, hence it has always same variance bound for a fixed set of parameters. The noise contained in a data element  $e_{data}$  is updated as  $e_{data} := c_1 \cdot e_{data} + c_2 \cdot v_q$  after one access, where  $c_1, c_2$  are small constants less than 5. Therefore, the noise (in terms of number of bits) grows with  $O(\log Q)$  complexity, where  $Q$  is the number of accesses. That is why we can keep small noise growth. Specifically, for  $n = 2^{19}, t = 2^8$  running Method 2 (Section 6) with batch size  $k = 256$ , and fixing our other parameters as described, we were able to process 425 successive batched queries, averaged after 10 samples, before we reached a decryption failure.

## 8 Limitations and Conclusion

This work introduces a novel ORAM paradigm which supports a stateless client and has a comparatively low bandwidth blowup; a major departure from the tree-based ORAM constructions in the existing literature. We propose our core protocol supporting single-access queries along with two variations for multi-access: The first variation uses parallelism to reduce the server’s computation time by 28% when compared to the core protocol; the second variation (Section 6) uses probabilistic batch codes to significantly improve the performance in the amortized setting (by over 180 times when compared to the core protocol for  $n = 2^{12}$ ), achieving only 1.16 seconds of access time for  $n = 2^{19}$ . However, we minimize the overheads on the client by increasing the overheads on the server, and that also brings some limitations:

- Although our asymptotic storage overhead on the server because of PBC is only a constant times (depending on the value of  $w$ ) more than that without PBC, the large size of FHE ciphertexts makes the overall concrete storage overhead high (with or without PBC). In practice, Path ORAM might consume less storage for the server. However, the storage overhead for Onion Ring ORAM remain similar to ours.

- Our client can only target distinct elements from the database in one batch. If a client would like to read, and then write based on what they read, they have to do that in two consecutive batches. This is a feature of RAM designs as opposed to alternative databases supporting prepared statements such as SQL.

- The asymptotic computation overhead on the server is linear in the number of elements in the database. While this asymptotic computation overhead for the server looks high compared to existing designs, our implementation’s concrete performance is more than acceptable, especially for small to moderately sized databases.

Our novel design approach invites other protocol designers to rethink the design space for ORAM. Investigating other amortization techniques that are compatible with stateless ORAM designs would be a very interesting future work. Another interesting future work would be to amortize and improve the overhead for the consistency correction step in our design.

## Acknowledgement

We thank the anonymous reviewers for their insightful comments. This work was carried out while Kelong Cong and Jeongeun Park were at COSIC, KU Leuven. The cloud resources and services used in this work were partly provided by the VSC (Flemish Supercomputer Center), funded by the Research Foundation - Flanders (FWO) and the Flemish Government. This work is partially supported by the Research Council KU Leuven under the grant C24/18/049, CyberSecurity Research Flanders with reference number VR20192203, and Defense Advanced Research Projects Agency (DARPA) under contract number FA8750-19-C-0502. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of any of the funders.

## References

1. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of learning with errors. *Journal of Mathematical Cryptology* 9(3), 169–203 (2015), <https://doi.org/10.1515/jmc-2015-0016>
2. Angel, S., Chen, H., Laine, K., Setty, S.T.V.: PIR with compressed queries and amortized query processing. In: 2018 IEEE Symposium on Security and Privacy. pp. 962–979. IEEE Computer Society Press (May 2018)
3. Angel, S., Setty, S.: Unobservable communication over fully untrusted infrastructure. In: 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16). pp. 551–569. USENIX Association, Savannah, GA (Nov 2016), <https://www.usenix.org/conference/osdi16/technical-sessions/presentation/angel>
4. Apon, D., Katz, J., Shi, E., Thiruvengadam, A.: Verifiable oblivious storage. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 131–148. Springer, Heidelberg (Mar 2014)
5. Chen, H., Chillotti, I., Ren, L.: Onion ring ORAM: Efficient constant bandwidth oblivious RAM from (leveled) TFHE. In: Cavallaro, L., Kinder, J., Wang, X., Katz, J. (eds.) ACM CCS 2019. pp. 345–360. ACM Press (Nov 2019)
6. Chen, H., Laine, K., Rindal, P.: Fast private set intersection from homomorphic encryption. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 2017. pp. 1243–1255. ACM Press (Oct / Nov 2017)
7. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 3–33. Springer, Heidelberg (Dec 2016)
8. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: TFHE: Fast fully homomorphic encryption over the torus. *Journal of Cryptology* 33(1), 34–91 (Jan 2020)
9. Chillotti, I., Joye, M., Ligier, D., Orfila, J.B., Tap, S.: Concrete: Concrete operates on ciphertexts rapidly by extending tfhe. In: WAHC 2020–8th Workshop on Encrypted Computing & Applied Homomorphic Cryptography. vol. 15 (2020)
10. Cong, K., Das, D., Park, J., Pereira, H.V.: Sortinghat: Efficient private decision tree evaluation via homomorphic encryption and transciphering. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. p. 563–577. CCS ’22, Association for Computing Machinery, New York, NY, USA (2022), <https://doi.org/10.1145/3548606.3560702>
11. Dautrich Jr., J.L., Stefanov, E., Shi, E.: Burst ORAM: Minimizing ORAM response times for bursty access patterns. In: Fu, K., Jung, J. (eds.) USENIX Security 2014. pp. 749–764. USENIX Association (Aug 2014)
12. Devadas, S., van Dijk, M., Fletcher, C.W., Ren, L., Shi, E., Wichs, D.: Onion ORAM: A constant bandwidth blowup oblivious RAM. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016-A, Part II. LNCS, vol. 9563, pp. 145–174. Springer, Heidelberg (Jan 2016)
13. Dietzfelbinger, M., Goerdt, A., Mitzenmacher, M., Montanari, A., Pagh, R., Rink, M.: Tight thresholds for cuckoo hashing via XORSAT. In: Abramsky, S., Gavoielle, C., Kirchner, C., Meyer auf der Heide, F., Spirakis, P.G. (eds.) ICALP 2010, Part I. LNCS, vol. 6198, pp. 213–225. Springer, Heidelberg (Jul 2010)
14. Fletcher, C.W., Ren, L., Kwon, A., van Dijk, M., Devadas, S.: Freecursive oram: [nearly] free recursion and integrity verification for position-based oblivious ram. *SIGPLAN Not.* 50(4), 103–116 (mar 2015), <https://doi.org/10.1145/2775054.2694353>
15. Frieze, A., Melsted, P., Mitzenmacher, M.: An analysis of random-walk cuckoo hashing. In: Dinur, I., Jansen, K., Naor, J., Rolim, J. (eds.) Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. pp. 490–503. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)

16. Garg, S., Mohassel, P., Papamanthou, C.: TWORAM: Efficient oblivious RAM in two rounds with applications to searchable encryption. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part III. LNCS, vol. 9816, pp. 563–592. Springer, Heidelberg (Aug 2016)
17. Geelen, R., Beirendonck, M.V., Pereira, H.V.L., Huffman, B., McAuley, T., Selfridge, B., Wagner, D., Dimou, G., Verbauwhede, I., Vercauteren, F., Archer, D.W.: BASALISC: Flexible asynchronous hardware accelerator for fully homomorphic encryption. Cryptology ePrint Archive, Report 2022/657 (2022), <https://eprint.iacr.org/2022/657>
18. Gentry, C., Goldman, K.A., Halevi, S., Jutla, C.S., Raykova, M., Wichs, D.: Optimizing ORAM and using it efficiently for secure computation. In: De Cristofaro, E., Wright, M.K. (eds.) PETS 2013. LNCS, vol. 7981, pp. 1–18. Springer, Heidelberg (Jul 2013)
19. Goldreich, O.: Towards a theory of software protection and simulation by oblivious RAMs. In: Aho, A. (ed.) 19th ACM STOC. pp. 182–194. ACM Press (May 1987)
20. Goldreich, O., Ostrovsky, R.: Software protection and simulation on oblivious RAMs. J. ACM 43(3), 431–473 (may 1996), <https://doi-org.kuleuven.e-bronnen.be/10.1145/233551.233553>
21. Goldreich, O., Ostrovsky, R.: Software protection and simulation on oblivious RAMs. J. ACM 43(3), 431–473 (may 1996), <https://doi.org/10.1145/233551.233553>
22. Goodrich, M.T., Mitzenmacher, M., Ohrimenko, O., Tamassia, R.: Privacy-preserving group data access via stateless oblivious RAM simulation. In: Rabani, Y. (ed.) 23rd SODA. pp. 157–167. ACM-SIAM (Jan 2012)
23. Hoang, T., Ozkaptan, C.D., Yavuz, A.A., Guajardo, J., Nguyen, T.: S<sup>3</sup>ORAM: A computation-efficient and constant client bandwidth blowup ORAM with shamir secret sharing. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 2017. pp. 491–505. ACM Press (Oct / Nov 2017)
24. Kushilevitz, E., Lu, S., Ostrovsky, R.: On the (in)security of hash-based oblivious RAM and a new balancing scheme. In: Rabani, Y. (ed.) 23rd SODA. pp. 143–156. ACM-SIAM (Jan 2012)
25. Larsen, K.G., Simkin, M., Yeo, K.: Lower bounds for multi-server oblivious RAMs. In: Pass, R., Pietrzak, K. (eds.) TCC 2020, Part I. LNCS, vol. 12550, pp. 486–503. Springer, Heidelberg (Nov 2020)
26. Lipmaa, H., Zhang, B.: Two new efficient pir-writing protocols. In: Zhou, J., Yung, M. (eds.) Applied Cryptography and Network Security. pp. 438–455. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
27. LLC, G.: All networking pricing — virtual private cloud — google cloud (2023), <https://cloud.google.com/compute/all-pricing>, accessed: May 2023
28. LLC, G.: Pricing — cloud storage — google cloud (2023), <https://cloud.google.com/compute/all-pricing>, accessed: May 2023
29. LLC, G.: Pricing — compute engine: Virtual machines (vms) — google cloud (2023), <https://cloud.google.com/compute/all-pricing>, accessed: May 2023
30. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (May / Jun 2010)
31. Mayberry, T., Blass, E.O., Chan, A.H.: Efficient private file retrieval by combining oram and pir. In: Network and Distributed System Security Symposium (2014), <https://api.semanticscholar.org/CorpusID:1542244>
32. Park, J., Tibouchi, M.: SHECS-PIR: Somewhat homomorphic encryption-based compact and scalable private information retrieval. In: Chen, L., Li, N., Liang, K., Schneider, S.A. (eds.) ESORICS 2020, Part II. LNCS, vol. 12309, pp. 86–106. Springer, Heidelberg (Sep 2020)
33. Pinkas, B., Schneider, T., Zohner, M.: Scalable private set intersection based on OT extension. Cryptology ePrint Archive, Report 2016/930 (2016), <https://eprint.iacr.org/2016/930>
34. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM) 56(6), 34 (2009)
35. Ren, L., Fletcher, C.W., Kwon, A., Stefanov, E., Shi, E., van Dijk, M., Devadas, S.: Constants count: Practical improvements to oblivious RAM. In: Jung, J., Holz, T. (eds.) USENIX Security 2015. pp. 415–430. USENIX Association (Aug 2015)
36. Samardzic, N., Feldmann, A., Krastev, A., Devadas, S., Dreslinski, R., Peikert, C., Sanchez, D.: F1: A fast and programmable accelerator for fully homomorphic encryption. In: MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture. p. 238–252. MICRO '21, Association for Computing Machinery, New York, NY, USA (2021), <https://doi.org/10.1145/3466752.3480070>
37. Shi, E., Chan, T.H.H., Stefanov, E., Li, M.: Oblivious RAM with  $O((\log N)^3)$  worst-case cost. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 197–214. Springer, Heidelberg (Dec 2011)
38. Stefanov, E., Dijk, M.V., Shi, E., Chan, T.H.H., Fletcher, C., Ren, L., Yu, X., Devadas, S.: Path oram: An extremely simple oblivious RAM protocol. J. ACM 65(4) (apr 2018), <https://doi.org/10.1145/3177872>
39. Stefanov, E., Shi, E.: ObliviStore: High performance oblivious cloud storage. In: 2013 IEEE Symposium on Security and Privacy. pp. 253–267. IEEE Computer Society Press (May 2013)

40. Stefanov, E., Shi, E., Song, D.X.: Towards practical oblivious RAM. In: NDSS 2012. The Internet Society (Feb 2012)
41. Stefanov, E., van Dijk, M., Shi, E., Fletcher, C.W., Ren, L., Yu, X., Devadas, S.: Path ORAM: an extremely simple oblivious RAM protocol. In: Sadeghi, A.R., Gligor, V.D., Yung, M. (eds.) ACM CCS 2013. pp. 299–310. ACM Press (Nov 2013)
42. Verma, P., Mathuria, A., Dasgupta, S.: Faster private rating update via integer-based homomorphic encryption. In: Tripathy, S., Shyamasundar, R.K., Ranjan, R. (eds.) Information Systems Security. pp. 218–236. Springer International Publishing, Cham (2021)
43. Wang, X., Chan, H., Shi, E.: Circuit oram: On tightness of the goldreich-ostrovsky lower bound. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. p. 850–861. CCS '15, Association for Computing Machinery, New York, NY, USA (2015), <https://doi.org/10.1145/2810103.2813634>
44. Wang, X.S., Huang, Y., Chan, T.H.H., shelat, a., Shi, E.: SCORAM: Oblivious RAM for secure computation. In: Ahn, G.J., Yung, M., Li, N. (eds.) ACM CCS 2014. pp. 191–202. ACM Press (Nov 2014)

## A Security

Here we revisit our security definition and theorems and provide the proofs.

### A.1 Security Definition

Recall that we adopt a standard security definition similar to [40,35].

**Definition 1** (Security Definition). *Let,*

$$\mathbf{y} := \{(\mathbf{a}_1, \text{op}_1, \text{data}_1), \dots, (\mathbf{a}_s, \text{op}_s, \text{data}_s)\}$$

*denote a sequence of data accesses by the client, where  $\mathbf{a}_i$  denotes the address of the block being read from or written to on the  $i$ -th access,  $\text{op}_i$  denotes the whether the operation on  $\mathbf{a}_i$  is a read or write,  $\text{data}_i$  denotes the data if the  $i$ -th operation is a write operation. Let  $A(\mathbf{y})$  denote the sequence of communication between the client and the server under an ORAM protocol  $\Pi$  for the access sequence  $\mathbf{y}$ . We say that  $\Pi$  provides security with correctness parameter  $\mu$ , if the following properties hold:*

**privacy:** *for any chosen pair of data access sequences  $\mathbf{y}$  and  $\mathbf{y}'$  of same length, the server cannot computationally distinguish between  $A(\mathbf{y})$  and  $A(\mathbf{y}')$ ;*

**correctness:** *for a sequence of input  $\mathbf{y}$ , the protocol returns output to the client consistent with  $\mathbf{y}$  with probability greater than  $1 - \mu$ .*

Note that the parameter  $\mu$  in our definition is not a negligible function in the asymptotic sense. Instead, we show concrete security for  $\mu \approx 2^{-40}$ , for the version with probabilistic batch codes (PBC). However, the version without PBC always returns the correct output as long as the underlying FHE scheme returns the correct output. Recall that we have an honest-but-curious server which can store all ciphertexts and other data sent by the client and, afterwards, act as a probabilistic polynomial time adversary to perform additional computations in order to infer the client’s private data or access patterns.

### A.2 Security Proof for $\text{Panacea}_{\text{core}}$

**Theorem 1** (Security of  $\text{Panacea}_{\text{core}}$ ). *Assuming IND-CPA security of the underlying FHE scheme  $\mathcal{E}$ , and assuming  $\mathcal{E}$  is correct except a failure probability negligible in the security parameter  $\lambda$ ,  $\text{Panacea}_{\text{core}}$  provides  $\mu$ -security as defined in Definition 1 with  $\mu$  negligible in  $\lambda$ .*

*Proof (Proof-sketch).* We perform the proof in two parts:

1. first, we show that it is difficult for the server to distinguish between two communication sequences corresponding to data access sequences  $\mathbf{y}$  and  $\mathbf{y}'$ , where  $|\mathbf{y}| = |\mathbf{y}'|$ ;
2. second, we show that the ORAM protocol always returns correct output and updates the accessed elements correctly.

*Claim.* Given two data access sequences  $\mathbf{y} = \{(a_1, \text{op}_1, \text{data}_1), \dots, (a_s, \text{op}_s, \text{data}_s)\}$  and  $\mathbf{y}' = \{(a'_1, \text{op}'_1, \text{data}'_1), \dots, (a'_s, \text{op}'_s, \text{data}'_s)\}$  of same length  $s \in \text{poly}(\lambda)$ , the server cannot (computationally) distinguish between communication sequences  $A(\mathbf{y})$  and  $A(\mathbf{y}')$  under the protocol  $\text{Panacea}_{\text{core}}$ .

*Proof:* Suppose, for the sake of contradiction, that the server can run a distinguisher  $\mathcal{D}$  to distinguish between  $A(\mathbf{y})$  and  $A(\mathbf{y}')$  with a probability  $p$  non-negligible in the security parameter  $\lambda$ .

We want to show that using this distinguisher  $\mathcal{D}$ , we can construct an adversary  $\mathcal{Adv}$  for the IND-CPA game of the underlying FHE scheme. For our proof we consider the IND-CPA game where the adversary is allowed to send multiple challenge queries.<sup>11</sup>

The adversary  $\mathcal{Adv}$  acts as the challenger in the ORAM security game against the server. The server can choose two sequences of data access  $\mathbf{y} = \{(a_1, \text{op}_1, \text{data}_1), \dots, (a_s, \text{op}_s, \text{data}_s)\}$  and  $\mathbf{y}' = \{(a'_1, \text{op}'_1, \text{data}'_1), \dots, (a'_s, \text{op}'_s, \text{data}'_s)\}$  of same length  $s$ . The challenger ( $\mathcal{Adv}$  in this case) picks one of  $\mathbf{y}$  and  $\mathbf{y}'$  based on the challenge bit  $b$  of the IND-CPA game and runs the ORAM protocol as described below:

1.  $\mathcal{Adv}$  allows the client to directly query the oracle of the IND-CPA game to receive encryptions for all database elements. The client provides the ciphertexts to  $\mathcal{Adv}$ , and  $\mathcal{Adv}$  provides them to the server to set up the database for the ORAM protocol.
2. After  $\mathcal{Adv}$  receives  $\mathbf{y}$  and  $\mathbf{y}'$  from the server, for each  $i \in [1, s]$ :
  - if  $a_i \neq a'_i$ ,  $\mathcal{Adv}$  uses  $a_i, a'_i$  as a pair of challenge plaintexts for the IND-CPA game and the response to construct the corresponding ORAM access request to the server;
  - if  $\text{op}_i \neq \text{op}'_i$ ,  $\mathcal{Adv}$  uses  $\text{op}_i$  and  $\text{op}'_i$  as a pair of challenge plaintexts for the IND-CPA game and the response to construct the corresponding request to the server;
  - if  $\text{data}_i \neq \text{data}'_i$ ,  $\mathcal{Adv}$  uses  $\text{data}_i, \text{data}'_i$  as a pair of challenge plaintexts for the IND-CPA game and the response to construct the corresponding request to the server;
  - $\mathcal{Adv}$  receives the ciphertexts corresponding to all remaining elements of  $\mathbf{y}$  (or  $\mathbf{y}'$ , since those elements are same) by querying the oracle of the IND-CPA game before sending the challenge pairs. Using them,  $\mathcal{Adv}$  can construct all  $s$  access requests.  $\mathcal{Adv}$  instructs the client to send the requests to the server.
3. Using the ciphertexts received from the IND-CPA game (as responses to the challenge pairs and oracle queries), the client runs the ORAM protocol with the server for  $s$  rounds.
4. If the distinguisher  $\mathcal{D}$  for the ORAM protocol returns 1,  $\mathcal{Adv}$  outputs 1 to the IND-CPA game.

Note that, whenever some parts of  $\mathbf{y}[i]$  and  $\mathbf{y}'[i]$  are different,  $\mathcal{Adv}$  (on behalf of the client for the ORAM protocol) chooses the corresponding ciphertext based on the response of the IND-CPA game. Therefore,  $\mathcal{Adv}$  effectively picks  $\mathbf{y}$  or  $\mathbf{y}'$  based on the challenge bit  $b$  of the IND-CPA game without actually knowing  $b$ .  $\mathcal{Adv}$  does not observe any of the database elements (during setup

<sup>11</sup> Security in a (polynomially bounded) multi-challenge IND-CPA game implies security in a single challenge IND-CPA game.

or the protocol run), or the actual queries in plaintext. Therefore, the server does not have any information other than the distinguisher  $\mathcal{D}$ , and the observed ciphertexts.

According to the ORAM protocol, the client sends all query elements  $(\mathbf{a}_i, \text{op}_i, \text{data}_i)$  as encrypted values. All database elements are also encrypted and all encrypted ciphertexts are re-randomized (as a result of operations under the FHE scheme) after every query. The response received by the client for each access is also encrypted.

For every access in ORAM, the server touches database elements: so that the access pattern is identical for every query.

This means that the distinguisher  $\mathcal{D}$  only has the ciphertexts that the client sends to the server or the results of homomorphic computations at its disposal. Therefore,  $\mathcal{A}$  wins the multi-query IND-CPA game with probability  $p$ . Which contradicts the IND-CPA security of the FHE scheme unless  $p$  is negligible.  $\diamond$

*Claim.* Given an input 3-tuple  $(\mathbf{a}, \text{op}, \text{data})$  to the ORAM access protocol, if any operations of  $\mathcal{E}$  does not return incorrect output, the client receives the correct response and the accessed element is correctly updated in case of a write operation.

*Proof:* The correctness of the ORAM protocol can be implied from: (1) correctness of the underlying FHE scheme, (2) the homomorphic traversal algorithm accessing the correct location, (3) the final step returning the correct value if the above conditions are satisfied, (4) and, if  $\text{op} = \text{Write}$ , the location is updated correctly.

By assumption of the claim, the FHE scheme is correct: all valid homomorphic operations will generate correct ciphertexts which can be correctly decrypted.

We can prove the correctness of homomorphic traversal by the method of induction on the number of database elements  $n$ . For simplicity, we assume  $n = 2^\ell$  for some integer  $\ell$ .

We first show, as the base case, that homomorphic traversal is correct for  $\ell = 1$ , i.e.,  $n = 2$ . In that case, the traversal tree consists of only the root and two leaves directly connected to the root. Before the traversal, the root contains the value  $b = 1$ , and each of the leaves contain  $\text{Enc}(0)$ . The client sends only one bit of  $\mathbf{a}$  (encrypted), which that acts as the controller bit for the root. Let us denote that encrypted controller bit with  $c$ . We update the right leaf node with  $b \cdot c$ , which is 1 if  $c = 1$ , and 0 otherwise (assuming the correctness of the FHE scheme). Similarly, the left node is updated with  $(1 - c) \cdot b$ , which is 1 if  $c = 0$ , and 0 otherwise.

Now, as an inductive hypothesis, let us assume that homomorphic traversal is correct up to a certain tree depth  $\ell$ . This means that for an  $\ell$ -bit  $\mathbf{a}$ , the traversal produces  $n = 2^\ell$  ciphertexts: of which  $n - 1$  are  $\text{Enc}(0)$ , and one is  $\text{Enc}(1)$  at index  $\mathbf{a}$ . We want to show that homomorphic traversal is correct for depth  $\ell + 1$ .

There are  $2^\ell$  nodes at the  $\ell$ -th level, and  $n = 2^{\ell+1}$  leaf nodes at level  $\ell + 1$ . Now,  $\mathbf{a}$  has  $\ell + 1$  bits. After,  $\ell$  iterations of the homomorphic traversal, all nodes at level  $\ell$  contain  $\text{Enc}(0)$ , except for one at location denoted by  $\mathbf{x} = \{\mathbf{a}[i]\}_{i \in [0, \ell-1]}$  which contains  $\text{Enc}(1)$  (by inductive hypothesis). Let us denote those nodes with  $b_i, i \in [0, 2^\ell - 1]$ ; for all  $i$ ,  $b_i = \text{Enc}(0)$  except  $b_x = \text{Enc}(1)$ . Consequently, during the  $(\ell + 1)$ -th iteration (which is also the last iteration), all leaf nodes will get the value  $\text{Enc}(0)$  except for the child nodes of  $b_x$ . We know from the structure of binary tree, that the child nodes of  $b_x$  are at indices  $x||0$  and  $x||1$  among the leaf nodes. Similar to the argument of base case, if  $\mathbf{a}[\ell + 1] = 0$ , then the left child is  $\text{Enc}(1)$  and the right child is  $\text{Enc}(0)$ , and vice-versa. Therefore, homomorphic traversal sets the correct element at depth  $\ell + 1$ .

Now the only thing remaining is to prove is that the final output is correct. Additionally, iff  $\text{op} = \text{Write}$ , then the database element is updated correctly with  $\text{data}$ . The first condition is implied by the correctness of the dot product between the output of the homomorphic traversal and the database element, which is in turn implied by the correctness of the FHE scheme. The second condition (correct update) is implied by the correctness of the RW and CMUX operations. RW ensures that the data element is updated iff  $\text{op} = \text{Write}$ , AND CMUX ensures that any update happens only at the location corresponding to the leaf with value  $\text{Enc}(1)$  after homomorphic traversal. The correctness of both of these operations are implied by the correctness of the FHE scheme.  $\diamond$

From the above claim we can say that  $\text{Panacea}_{\text{core}}$  always returns the correct result for all possible sequence  $\mathbf{y}$  if  $\mathcal{E}$  is correct. However, if  $\mathcal{E}$  has a negligible failure probability  $\gamma$ ,  $\text{Panacea}_{\text{core}}$  has a negligible failure probability of  $\mu = \text{poly}(\gamma)$ , since  $s \in \text{poly}(\lambda)$ .  $\square$

### A.3 Security Proof for $\text{Panacea}_{\text{pbc}}$

**Theorem 2** (Security of  $\text{Panacea}_{\text{pbc}}$ ). *Let  $\mathcal{E}$  be an IND-CPA secure FHE scheme that is correct except with a failure probability  $\gamma \in \text{negl}(\lambda)$ . Given a sequence of data accesses  $\mathbf{y} = \{(\mathbf{a}_1, \text{op}_1, \text{data}_1), \dots, (\mathbf{a}_s, \text{op}_s, \text{data}_s)\}$  of length  $s \in \text{poly}(\lambda)$ , with each batch of size  $k$ , and a failure probability  $p$  of the probabilistic batch code,  $\text{Panacea}_{\text{pbc}}$  provides security as defined in Definition 1 with the correctness parameter  $\mu < p \cdot \frac{s}{k} + \text{negl}(\lambda)$ .*

*Proof (proof-sketch).* Similar to the proof of Theorem 1, we also provide this proof in two parts:

1. we show that it is difficult for the server to distinguish between two communication sequences corresponding to data access sequences  $\mathbf{y}$  and  $\mathbf{y}'$ , where  $|\mathbf{y}| = |\mathbf{y}'|$ ;
2. we show that the ORAM protocol returns correct output with a probability very close to 1.

We will first prove our second claim, then prove the first one. For simplicity, since the client always sends queries in batches of size  $k$ , we assume that  $s = \alpha k$  where  $\alpha$  is an integer. A similar argument can be extended easily for other values of  $\alpha$  assuming that the client will add dummy access requests to complete the size  $k$  of the last batch.

*Claim.* Given a sequence of inputs  $\mathbf{y} = \{(\mathbf{a}_1, \text{op}_1, \text{data}_1), \dots, (\mathbf{a}_s, \text{op}_s, \text{data}_s)\}$  to the ORAM access protocol, if any operations of  $\mathcal{E}$  does not return incorrect output, the access operations (read or write) are correctly executed for all the input tuples  $(\mathbf{a}_i, \text{op}_i, \text{data}_i)$  with probability  $1 - \mu$  where  $\mu < p \cdot \frac{s}{k}$ .

*Proof:* In the proof of Appendix A.2 we have argued that the homomorphic traversal yields the correct output. However,  $\text{Panacea}_{\text{pbc}}$  additionally applies batching, and individually runs  $\text{Panacea}_{\text{core}}$  over each of the  $b$  buckets. Therefore, we can argue that each individual run over all buckets preserves correctness with 0 failure probability, when an access request is made by the client.

However, the batching technique comes with a failure probability  $p$ : for a (randomly chosen) batch of size  $k$ , the client will fail to create a batch which can retrieve all  $k$  elements with probability  $p$ . In such a case, we consider that our ORAM protocol has failed to generate the correct output.

For a sequence of length  $s$ , there is a total of  $\frac{s}{k} = \alpha$  batches. The probability that none of them fails is quantified by:

$$P = (1 - p)^\alpha \geq 1 - \alpha p$$

Therefore, the probability that at least one of them fails is quantified by:

$$\mu = 1 - P \leq \alpha p$$

If all batches are successful, then the client retrieves correct output for all access requests in the sequence  $\mathbf{y}$  (implied from the success condition of the batching and correctness of the FHE scheme). The client fails to retrieve all the  $s$  elements if one of the batches fails; which happens with probability  $\mu \leq \alpha p = p \cdot \frac{s}{k}$ .  $\diamond$

However, there is a negligible probability  $\gamma$  for the FHE scheme to generate incorrect results. In such cases, the client will receive inconsistent output. Since  $\gamma \in \text{negl}(\lambda)$  and  $s \in \text{poly}(\lambda)$ ,  $\mu \leq p \cdot \frac{s}{k} + \gamma \cdot \text{poly}(s) \leq p \cdot \frac{s}{k} + \text{negl}(\lambda)$ .

Now we move to proving the first claim which states that two communication sequences  $A(\mathbf{y})$  and  $A(\mathbf{y}')$  corresponding to  $\mathbf{y}$  and  $\mathbf{y}'$  are indistinguishable by the server. However, to ensure that no leakage emerges from the number of batches actually requested by the client, in case there is a failure with PBC, we assume that the client completes the batch with dummy requests and sends the batch even if this action would not help the client retrieve/update the  $k$  elements. With that additional assumption, we can claim the following:

*Claim.* Given two sequences of accesses  $\mathbf{y} = \{(a_1, \text{op}_1, \text{data}_1), \dots, (a_s, \text{op}_s, \text{data}_s)\}$  and  $\mathbf{y}' = \{(a'_1, \text{op}'_1, \text{data}'_1), \dots, (a'_s, \text{op}'_s, \text{data}'_s)\}$  of same length  $s$ , the server cannot (computationally) distinguish between the communication sequences  $A(\mathbf{y})$  and  $A(\mathbf{y}')$  under the protocol  $\text{Panacea}_{pbc}$ .

*Proof:* The proof of this claim is very similar to that of Appendix A.2. The only difference is that the queries are now sent in batches of  $k$ ; but nevertheless, the server still touches all the elements in the database for each batch. Same as in the proof of Appendix A.2, the server can break the IND-CPA game for the underlying FHE scheme if the security of the ORAM scheme is broken.

The server can choose two sequences with one different element (which is at position  $s$ ):  $(a_i, \text{op}_i, \text{data}_i) = (a'_i, \text{op}'_i, \text{data}'_i) \forall 1 \leq i \leq (s-1)$ , but  $a_s \neq a'_s$  and  $\text{data}_s \neq \text{data}'_s$ ; however, the server picks  $\text{op}_s = \text{op}'_s$ . The server picks either  $\text{op}_s = \text{Read}$  or  $\text{Write}$  uniformly at random. Then the server tries to distinguish which one of  $\mathbf{y}$  and  $\mathbf{y}'$  is chosen by the client.

The server plays two IND-CPA games  $\mathcal{G}_1$  and  $\mathcal{G}_2$  as an adversary. In  $\mathcal{G}_1$ , the server chooses the pair  $(a_s, a'_s)$  as challenge plaintexts for the IND-CPA game, and in  $\mathcal{G}_2$  the pair  $\text{data}_s$  and  $\text{data}'_s$  as challenge plaintexts. If the distinguisher  $\mathcal{D}$  for the ORAM protocol returns 1, the server outputs 1 to both games. We skip the detailed proof here.  $\diamond$

From the above two claims we can claim that  $\text{Panacea}_{pbc}$  provides security as defined in Definition 1 with  $\mu \leq p \cdot \frac{s}{k} + \text{negl}(\lambda)$

In our batching technique with PBC, we choose parameters such that  $p \approx 2^{-40}$ . That makes  $\mu \approx 2^{-40} \times \frac{s}{k}$ . Even after a million batch queries (with each batch containing  $k$  queries), the probability that any of the batches would fail is almost one-in-a-million.

#### A.4 Defense Against Malicious Servers

The design presented in this paper mainly focuses on an honest but curious server (adversary). Our design can be extended with minor modifications to support the assumptions required when considering a malicious server. We use a technique similar to [14], where the client stores message authentication codes along with the elements. More specifically, for every element  $d_i$  the client stores  $\text{Enc}(d_i, \text{MAC}_K(i, d_i))$  at slot  $i$  in the database. This allows the client to immediately detect if the server does not follow the protocol and returns a bad ciphertext or a ciphertext from any location other than the queried index for a  $\text{Read}$  access. However, the server might still be able to replay old elements from the same location. One way to mitigate against replay attacks, and guarantee



the freshness of the blocks, would be to maintain a separate counter for each element, and use that counter as part of the input of MAC. After every Write access the corresponding counter needs to be increased. However, this requires that client maintains a state of all the counters locally, which adds state to our stateless design.

So we suggest a probabilistic defense mechanism: For every  $t$  Write accesses, the client chooses one of them at random for verification purposes. The index corresponding to that verification access would be Read immediately after a Write operation at the same location. If the server's response does not match the previously updated value on the position, then the client can immediately detect the server's malicious behavior. Our privacy guarantees imply that the server cannot learn anything about the type of intended access, as such, the server has no way to infer access patterns to identify the for verification accesses. For every malicious action, the client detects it with a probability of at least  $\frac{1}{t}$ .

When the client detects such a malicious action by the server, if the client aborts immediately, that provides a unique side-channel to the server. The server knows that after (maliciously) modifying a certain block the client has aborted the protocol. We leave it for future work to handle such side-channel attacks. However, the server will try to avoid detection for financial purposes, e.g., if it is a cloud server running storage as a service. If the clients can detect such malicious behavior from the server, they will eventually take their businesses elsewhere.

## B Query Unpacking

In this section, we discuss how to pack a query for slower noise growth, while keeping a practical computation time. Algorithm 3 of [5] has the least computation complexity among the conversion methods from  $\text{RLWE}(M(X))$  to  $\text{RLWE}(M_i)$ , where  $i \in [N]$  with  $\mathcal{O}(\log N)$  complexity. However, this approach results in a lot of noise at the end as discussed in their paper. Therefore, we slightly modify the algorithm by adopting a key switching method (Algorithm 7 of [5]).

Before discussing the algorithm, we define below a ciphertext form which we will employ:

- $\text{RLWE}'_s(m) := \mathbf{Z} + (0, \mathbf{g} \cdot m \in R_q^{\ell \times 2})$ , where  $\mathbf{Z}$  is a matrix where each row is an  $\text{RLWE}_s(0)$ , and  $\mathbf{g} := (b^0, b^1, \dots, b^{\ell-1})^t$  for a positive integer  $b$ . The secret key  $s$  is defined as  $s_0 + s_1X + \dots + s_{N-1}X^{N-1}$ .

Our query consists of  $C := \text{RLWE}(M(X))$  packing all bits in coefficients of  $M(X)$ . Then we rearrange the coefficient of  $C$  to place the desired coefficient at the constant term. Next, we run the following key switching algorithm to output  $C_i := \text{RLWE}(M_i)$ .

---

### Algorithm 7 Key Switching from an RLWE to an RLWE

---

**Input:**  $\mathbf{c} := \text{RLWE}_s(M(X)) = (a, b)$ , where  $b = -a \cdot s + \Delta M(X) + e$ , and  $\text{ksk} := \{\text{ksk}_i := \text{RLWE}'_s(s_i)\}_{i \in [0, \dots, N]}$

**Output:**  $c := \text{RLWE}_s(M_0) \in R_q^2$

- 1: Parse  $a := a_0 + a_1X + \dots + a_{N-1}X^{N-1}$
  - 2: **for**  $i \leftarrow 1$  to  $N$  **do**
  - 3:     Compute  $c_i := (\langle \mathbf{g}^{-1}(a_i), \text{ksk}_i[1] \rangle, \langle \mathbf{g}^{-1}(a_i), \text{ksk}_i[2] \rangle)$
  - 4: Compute  $c := (\sum_{i=1}^n c_i[1], b + \sum_{i=1}^n c_i[2])$
  - 5: **return**  $c$
- 

Then, we switch the call of Algorithm 3 by the above algorithm in Algorithm 4 of Onion Ring ORAM to generate the same output.

The algorithm consists of  $N$  scalar products between an integer and polynomial, which costs less than  $N$  external products, with additive noise growth. Consequently, the output noise only has  $N$  factor in the variance, whereas Algorithm 3 incurs a factor of  $N^2$ .

## C Deployment Strategy

### C.1 Response Time Improvement from Cloud Orchestration

Till now we have assumed that a single server holds all the buckets. However, if we consider a cloud service scenario, each of the  $b$  buckets can be held by a different cloud server, employing a total of  $b$  cloud servers. However, after the response is sent to the client, one of them still needs to run the consistency correction for the whole database, and communicate the updates to rest of the servers— which adds additional intra-cloud communication. In our evaluation in Appendices C.2 and C.3 we consider the following setting: there is one persistent database instance  $D$ , and spawn  $(b - 1)$  additional on-demand instances to process each bucket; once the buckets are processed,  $D$  runs the consistency correction for the whole database. We demonstrate that such a setting can yield an overall response time (for the whole batch) close to the amortized response time; and does not incur significant cost for the intra-cloud communication. We would like to emphasize that this orchestration does not change our security model: all cloud resources would be under the control of one entity, e.g., Amazon AWS or Google Cloud.

### C.2 On-Demand Server

Instead of having a long-running server, cloud services can be used to create on-demand servers for the majority of the processing requirements. In our case, the client stores the database in a Google Cloud Storage Bucket. Whenever a query (or a batch of them) is submitted by a client, it would be ingested by a cloud scheduler, operating at negligible cost, which boots up an instance of our server from a snapshot. This instance would exist only for the duration of performing one access operation, to minimize billing costs. The server instance, provided with the client’s query by the scheduler, would then fetch the required database bucket and parameters from the storage bucket and store them directly to on its ramdisk partition.

We assume that the speed at which the ramdisk partition on the server can communicate bi-directionally with the storage solution at a rate of 4GB/s<sup>12</sup>. The server instance then computes the response, transmits it back to the client, updates the database and stores it back on the storage solution then gets shut down automatically. For batch processing, the cloud scheduler can spawn  $b$  such instances (one corresponding to each bucket); once each of those instances finishes their processing, the scheduler spawns another separate instance to run the consistency correction on the whole database. The total billable time during which our server operates can be calculated by summing the time to load the encrypted database, the total computation time and the time to store the updated database.

### C.3 Monetary Cost

Using the same parameter set from Table 3 and  $k = 256$ , we present the concrete cost of operating our server using Method 2 without query packing. Appendix D provides a reference price list retrieved from the website of Google Cloud Platform (GCP) [27,28,29].

<sup>12</sup> <https://cloud.google.com/compute/docs/disks/performance>

Table 6: Growth of database in GB with  $n$  from  $2^{12}$  to  $2^{19}$  and estimated cost of storage per month in US Dollars

$n$	Database Size (GB)	Cost per Month
$2^{12}$	0.403	\$0.010478
$2^{14}$	1.611	\$0.041886
$2^{16}$	6.445	\$0.16757
$2^{18}$	25.782	\$0.670332
$2^{19}$	51.564	\$1.340664

Table 7: Server time to load the database from storage, perform the ORAM computation, store the updated database in storage, and their sum (total server time) in seconds with the estimated monetary cost in US Dollars.

$n$	Load	ORAM	Update	Total	Cost
$2^{12}$	0.1	3.48	0.1	3.68	\$0.02576
$2^{14}$	0.402	12.42	0.402	13.2	\$0.092568
$2^{16}$	1.611	49.13	1.611	52.35	\$0.366464
$2^{18}$	6.445	195.94	6.445	208.83	\$1.46181
$2^{19}$	12.891	391.26	12.891	417.042	\$2.919294

**Data Transfer and Storage.** Given that internal storage traffic (i.e. transfers between a cloud instance and a standard storage bucket) is free of charge on GCP, we can neglect the monetary cost of transferring the database from client to server. The same applies for Ingress traffic from the client to the cloud, which means that the client can transmit their queries with no server-side cost.

Our fixed parameters grant us a fixed server response size of 12.5MB, regardless of the database size. This translates to \$0.0028 of billable egress traffic per response. Table 6 shows the of the database to be stored size in GB with  $n$  from  $2^{12}$  to  $2^{19}$  and the estimated cost in US Dollars per month. This low cost demonstrates that storing, transferring and treating FHE ciphertexts is affordable for significantly-scaled server deployments.

**Server-Side Protocol Execution.** We assume that our server runs on demand. More details on our proposed server setup can be found in Appendix C.2. For simplicity, we assume that regardless of the value of  $n$ , a server instance would be equipped with 36 cores and 2TB of RAM to replicate our experimental setup. Thus referring to Table 8 we can assume that running our server would cost \$25.2/h or \$0.007/s. Table 7 provides an estimated cost in US Dollars per batch of 256 queries with  $n$  from  $2^{12}$  to  $2^{19}$ .

## D Google Cloud Platform Reference Price List

The price list from Google Cloud Platform [27,28,29] is added in Table 8 for reference.

Table 8: Cloud services required and reference unitary price list from Google Cloud Platform (GCP) in US Dollars for Europe region

<b>Service</b>	<b>Unit</b>	<b>Price/Unit</b>
Standard Storage	GB/month	\$0.026
Storage Traffic	GB	Free
Memory-optimized Compute CPU	Core/hour	\$0.03831
Memory-optimized Compute Memory	GB/hour	\$0.00563
Premium Ingress Traffic	GB	Free
Premium Egress Traffic	GB	\$0.23