Time- and Space-Efficient Aggregate Range Queries over Encrypted Databases

Abstract: We present ARQ, a systematic framework for creating cryptographic schemes that handle range aggregate queries (sum, minimum, median, and mode) over encrypted datasets. Our framework does not rely on trusted hardware or specialized cryptographic primitives such as property-preserving or homomorphic encryption. Instead, ARQ unifies structures from the plaintext data management community with existing structured encryption primitives. We prove how such combinations yield efficient (and secure) constructions in the encrypted setting. We also propose a series of domain reduction techniques that can improve the space efficiency of our schemes against sparse datasets at the cost of small leakage. As part of this work, we designed and implemented a new, open-source, encrypted search library called Arca and implemented the ARQ framework using this library in order to evaluate ARQ’s practicality. Our experiments on real-world datasets demonstrate the efficiency of the schemes derived from ARQ in comparison to prior work.

Keywords: structured encryption, encrypted search algorithms, aggregate queries, range queries

1 Introduction

Structured encryption (STE) [15, 17] refers to a class of encrypted search algorithms (ESA) [29, 42] that allow a client to outsource (and query) an encrypted version of their data to a semi-honest server. Recent research in STE has focused on developing specialized structures that efficiently handle more expressive types of queries, such as range queries. For example, the BlindSeer construction from [57], the garbled-circuit-based construction from [10], and the range tree constructions from [19, 20, 25, 27, 49, 65, 68] are all examples of encrypted range query structures. In these works, range queries are effectively a simple filter, applied to a single database attribute, that returns a set of matching records.

Aggregate range queries. Despite the focus on encrypted range structures in recent years, real-world applications often do not directly require the records in the queried range, but rather the result of an aggregate function folded over a second record attribute in the queried range. Consider, for instance, the following SQL query over an employees table, which asks for the median salary of all employees between the ages 30 and 40:

```sql
SELECT MEDIAN(salary) FROM employees WHERE age BETWEEN 30 AND 40;
```

We call the attribute the filter is composed over the filter attribute and the attribute the aggregation function is composed over the aggregate attribute. In this example, the filter attribute is age and the aggregate attribute is salary. To answer this query, the server only needs to output a single numerical value (the median salary). Integrating aggregate functions directly into queries in this way can minimize bandwidth as the server only needs to send a constant-size value to the client.

Performance gap for encrypted aggregates. Using existing record-reporting STE schemes to answer aggregate queries over encrypted data incurs a significant overhead. In many STE structures, the server cannot compute the aggregate server-side and must return the entire set of records satisfying the filter. This incurs linear-size bandwidth and requires the client to spend linear resources to decrypt each of the records before computing the aggregate. Conversely, one may precompute answers to all possible range queries in an encrypted dictionary. This achieves constant-size bandwidth and query time, but prohibitively requires quadratic storage.

Many approaches have been proposed to bridge this performance gap. Fully homomorphic encryption (FHE) [30], for example, can allow the server to compute portions of the aggregate before responding to the client. Unfortunately, state-of-the-art FHE schemes have high performance costs and are prohibitive for real-world
applications. As an alternative, additively homomorphic encryption (AHE) [56] imposes more acceptable performance costs and allows the server to sum encrypted values prior to sending them to a client. However, AHE does not allow for non-additive aggregates (e.g., min/max) and still requires the server to spend computation time to add AHE ciphertexts.

Alternatively, some encrypted range structures can be augmented with precomputed sub-aggregates within the structure. Queries may then be answered by returning a poly-logarithmic set of sub-aggregates which the user processes to recover a single aggregate. These schemes can be somewhat more practical for aggregate queries; however, they may incur higher than necessary storage overhead, especially when the dataset is sparse.

Aside from performance concerns, “naive” STE approaches for handling aggregates may incur more leakage than necessary. While the ultimate goal of the end user is to compute a single aggregate value, using standard record-reporting STE schemes as a building block for aggregates often results in search pattern leakage (whether the same query is made multiple times) and access pattern leakage (whether the same encrypted record is used to respond to multiple queries) that may eventually lead to reconstruction attacks [7, 42]. These performance and security limitations highlight the need for new constructions for encrypted range aggregates.

**Contributions.** We take an interdisciplinary approach and demonstrate how simple combinations of data structures previously developed in the plaintext data management community with STE primitives can yield efficient (and secure) constructions in the encrypted setting. More generally, our work aims to showcase how cryptographers can leverage prior advances in databases and data structures to develop secure constructions for ESAs. Our contributions are summarized as follows:

- We introduce ARQ, a framework for building encrypted aggregate range query indexes which provably captures the leakage of our schemes. We identify a data-oblivious (DO) security property which guarantees that data reconstruction attacks are impossible against DO schemes, provided that query and data distributions are independent. (§ 3, § 4)
- Using ARQ, we propose novel schemes for encrypted range minimum, approximate mode, and approximate median. Denoting with $m$ the domain size (number of possible values of the filter attribute) and with $n$ the number of records, our minimum scheme improves the previous best $O(m + n \log n)$ storage of Demertzis et al.’s 2-round protocol [20] to an $O(m)$ storage 1-round protocol by prohibiting some small queries. To our knowledge, our approximate mode and median schemes are the first in the STE literature and allow for constant time and size queries. (§ 5, § 6, § 7)
- We propose domain reductions which can be applied to any ARQ scheme to optimize its storage overhead over sparse databases in exchange for small performance and leakage. Our reductions improve the performance of the sum and minimum constructions by Demertzis et al. [20] over sparse databases. (§ 8)
- We implement Arca, a new Python library for rapid prototyping of ESAs using STE schemes. Using Arca, we provide a reference implementation of the ARQ framework in Python. Using this implementation, we conduct an empirical evaluation of our proposed schemes against real-world datasets. (§ 9)

## 2 Related Work

**Encrypted range aggregate queries in STE.** Demertzis et al. [20] introduced the first study of STE structures for encrypted range sum and minimum queries with constant client-side storage, bandwidth, and computation time. They proposed an encrypted range sum scheme based upon the classic prefix sums technique [9]; it requires $O(m)$ storage, where $m$ is the domain size (number of possible values of the filter attribute). They also proposed two schemes for encrypted range minimums based upon the sparse table technique by Bender et al. [5]. The first scheme incurs $O(m \log m)$ storage in the size of the domain. The second scheme incurs a smaller $O(m + n \log n)$ storage requirement, where $n$ is the number of records, at the expense of an additional round trip. However, even with the storage optimization of the second scheme, the $O(m)$ factor in the asymptotics still may be prohibitive for sparse databases.

**Encrypted aggregates via other techniques.** Many works have been proposed to support aggregate functions over encrypted databases via various forms of homomorphic encryption and property preserving encryption. A notable example is CryptDB, the first system to support standard SQL operations over encrypted data [60]. CryptDB uses specialized encryption schemes such as order-preserving encryption (OPE) [11] and additively homomorphic encryption (AHE) [56] to support certain SQL operations, including aggregates. Many similar works use AHE to support aggregates [3, 34, 40, 43, 62].
Table 1. Our contributions compared to Demertzis et al. (DPPDGP) [20]. Storage, query time, and communication bandwidth are asymptotic (big-Ω), where \( m \) is the domain size, \( n \) is the number of records, and \( 0 < \alpha < 1 \) is a tunable parameter. Storage and query time are given separately for the server and the client. We further characterize tradeoffs between the schemes by indicating whether a scheme is data-oblivious (“DO”) (Definition 3.3) or optimizes storage by taking advantage of sparsity in datasets (“Sparse”).

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Server Complexity</th>
<th>Communication</th>
<th>Client Complexity</th>
<th>Tradeoff</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Storage</td>
<td>Query</td>
<td>Bandwidth</td>
<td>Rounds</td>
</tr>
<tr>
<td>Sum</td>
<td>( m )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Sum + DomainBucket</td>
<td>( m^\alpha + n )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Sum + DataBucket</td>
<td>( m^\alpha + n )</td>
<td>1</td>
<td>( n/m )</td>
<td>1</td>
</tr>
<tr>
<td>Minimum</td>
<td>( m \log m )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DPPDGP-Min1 [20]</td>
<td>( m + n \log n )</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>LinearMin</td>
<td>( m )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Mode</td>
<td>( m \log m )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1/2-ApproxMode</td>
<td>( m \log m )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1/3-ApproxMode</td>
<td>( m \log m )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Median</td>
<td>( \alpha )-ApproxMedian</td>
<td>( m )</td>
<td>( 1/\alpha )</td>
<td>1</td>
</tr>
</tbody>
</table>

However, AHE does not support non-additive aggregate queries, so many of these works do not support operations such as minimum, median, and mode. Additionally, while OPE may be used for rank-based range aggregates (e.g., median), many works have demonstrated that OPE leaks enough information to allow for powerful, practical data-recovery attacks [6, 21, 38, 53]. Other works rely on trusted hardware. For instance, Cipherbase supports aggregations using custom, trusted field-programmable gate arrays (FPGAs) [3] that are used to compute sum aggregates. It sends encrypted values to the FPGAs to be decrypted and summed. Then, the result is reencrypted before releasing it to the untrusted environment. Other works use trusted execution environments such as Intel SGX. However, the security guarantees of such hardware are complex and often are memory-limited. We do not rely on specialized hardware or hardware security assumptions in this work.

Leakage-abuse attacks on encrypted range structures. An important property of a structured encryption scheme is its leakage, or what information is revealed by the scheme’s operations. Islam et al. introduced the first study of STE leakage-abuse attacks [41]; they showed how to perform query-recovery attacks by exploiting access pattern leakage. Follow-up work such as Cash et al. [13] and Zhang et al. [67] exploited access pattern leakage to launch query-recovery attacks with similar impact under different assumptions. Recent work has also shown how to combine access and search pattern leakage to perform query-recovery attacks [55].

The increased expressiveness of range queries may allow for more severe data-recovery attacks. Many works have demonstrated powerful one-dimensional attacks under varying assumptions (see, e.g., [36, 37, 39, 45–48]), and a recent line of work has yielded reconstruction attacks in higher dimensions [26, 27, 50]. The impact of these kinds of attacks can vary when pitted against real-world datasets and query distributions [42].

3 Preliminaries

Notation. \( \{0,1\}^\ell \) denotes the set of all binary strings of length \( \ell \). \( \{0,1\}^* \) denotes the set of all finite binary strings. \( \bot \) represents the empty string. \( x \leftarrow A \) represents the output of procedure \( A \). Given a set \( S \), the cardinality of \( S \) is denoted \( |S| \). The set of numbers \( \{0,1,\ldots,x-1\} \) is denoted \( [x] \).

Basic structures. Our protocols use several basic data structures whose syntax we define here. A dictionary \( DX \) of size \( s \) is a collection of \( s \) key-value pairs. \( v_i := DX[\ell_i] \) denotes the retrieval of the value \( v_i \) associated with the label \( \ell_i \). \( DX[\ell_i] := v \) denotes the assignment of value \( v \) to label \( \ell_i \). A multimap \( MM \) of size \( s \) is a collection of \( s \) key-tuple pairs. \( t_i := MM[\ell_i] \) denotes the retrieval of the tuple \( t_i \) associated with the label \( \ell_i \). \( MM[\ell_i] := t_i \) denotes the assignment of tuple \( t_i \) to label \( \ell_i \). The length of each tuple \( t_i \) may vary within the multimap.

Given a data structure \( DS \), we refer to the act of retrieving the value associated with a label in \( DS \) as querying \( DS \). We refer to the set of labels that can be used to query \( DS \) as the query space of \( DS \) and the set of possible outputs as the response space of \( DS \). We write \( DS : Q \rightarrow R \) to denote that \( Q \) is \( DS \)'s query space and \( R \) is \( DS \)'s response space. We denote the number of key-value pairs in \( DS \), or \( DS \)'s size, as \( |DS| \).
Tables. A table \(DB\) is a two-dimensional array where each row is a record and each column is an attribute. We assume that each attribute has a finite domain of possible values. Every record \(r \in DB\) is a tuple indexed by each of \(DB\)'s attributes. In this work, we primarily consider one-dimensional queries, so we assume that every record has one filter attribute and one aggregate attribute for simplicity. Given a domain value \(x_i\), we use \(DB(x_i)\) to denote the set of records with filter attribute value \(x_i\). We also use \(DB^{-1}(x_i)\) to denote the record with filter attribute value closest or equal to, but not greater than, \(x_i\); similarly, \(DB^+ (x_i)\) denotes the record with filter attribute value closest to, but not less than, \(x_i\).

Throughout the paper, we use \(n\) to refer to the number of records in \(DB\) and \(m\) to refer to the domain size of \(DB\)'s filter attribute.

Structured encryption. A structured encryption (STE) scheme encrypts a data structure \(DS\) so that a client can outsource it and privately query it using a secret key \(K\). We exclusively use response-hiding schemes where query responses are not revealed to the server.

**Definition 3.1** (Response-hiding STE [15]). A STE scheme \(\Sigma = (\text{Setup}, \text{Token}, \text{Query}, \text{Resolve})\) consists of four polynomial-time algorithms that work as follows:

- \((K, EDS) \leftarrow \text{Setup}(1^k, DS)\) is a probabilistic algorithm run by the client. It takes as input a security parameter \(1^k\) and a plaintext data structure \(DS\). It then outputs a key \(K\) and an encrypted structure \(EDS\).
- \(tk \leftarrow \text{Token}(K, Q)\) is a deterministic algorithm run by the client when it issues a query. It takes as input a key \(K\) and a query \(Q\) and outputs a token \(tk\).
- \(ct \leftarrow \text{Query}(EDS, tk)\) is a deterministic algorithm run by the server to respond to queries. It takes as input the encrypted structure \(EDS\) and a query token \(tk\) and outputs a response \(ct\) (which may be \(\perp\)).
- \(R \leftarrow \text{Resolve}(K, ct)\) is a deterministic algorithm that takes as input the secret key \(K\) and a ciphertext \(ct\) and outputs a plaintext response \(R\).

We say \(\Sigma\) is correct if, for all \(k \in \mathbb{N}\), for all poly\((k)\)-size structures \(DS : Q \rightarrow R\), for all poly\((k)\)-size sequences of queries \(Q_1, \ldots, Q_m\) where \(Q_i \in Q\), for all \(tk_i\) output by \(\text{Token}(K, Q_i)\), \(\text{Resolve}(K, \text{Query}(EDS, tk_i)) = DS[Q_i]\) with all but negligible probability.

Definition 3.1 applies to non-interactive STE schemes. Some STE protocols are interactive, where queries client involve more than one round of communication.

**Definition 3.2** (Interactive STE). A interactive STE scheme \(\Sigma = (\text{Setup}, \text{Query})\) consists of two polynomial-time algorithms where \(\text{Setup}\) is the same as it was in Definition 3.1 and \(\text{Query}\) is as follows:

- \((R, \perp) \leftarrow \text{Query}_{C,S}(\langle K, Q \rangle, EDS)\) is a two party protocol algorithm run between the client and the server. It takes as input from the client a key \(K\) and a query \(Q\) and as input from the server an encrypted structure. It outputs a plaintext result \(R\) to the client and nothing to the server.

We say \(\Sigma\) is correct if, for all \(k \in \mathbb{N}\), for all poly\((k)\)-size structures \(DS : Q \rightarrow R\), for all poly\((k)\)-size sequences of queries \(Q_1, \ldots, Q_m\) where \(Q_i \in Q\), \(\text{Query}_{C,S}(\langle K, Q_1 \rangle, EDS) = DS[Q_i]\) with all but negligible probability.

**Security definitions.** To prove security of an STE protocol \(\Sigma\), we define leakage functions that capture what information is revealed by the different operations of \(\Sigma\): \(L_S\), the setup leakage, or what is leaked by the \(\text{Setup}\) operation, and \(L_Q\), the query leakage, or what is leaked by the \(\text{Query}\) algorithm. We then prove that a semi-honest, adaptive adversary can only distinguish between two experiments with negligible probability: the real world, in which the actual STE protocol is used against the adversary, and the ideal world, which attempts to simulate the real world only based on the leakage \(L_S\) and \(L_Q\). We use the standard definitions for adaptive semantic security from [15], which we recap in Appendix A.

### 3.1 Data-Oblivious STE Schemes

In our work, we find that the reduced expressiveness of aggregate structures (they do not return the records in the queried range) means that aggregate structures do not necessarily suffer from the same types of leakage as SSE structures (i.e., volume pattern, search pattern, and access pattern to individual records). As such, we are interested in precisely capturing when such a scheme avoids these kinds of data-dependent leakage patterns, as this would imply that the scheme is secure against all previously known data-reconstruction attacks.

We call this property data-obliveness (DO). This property is similar to the standard definition used in the data-oblivious algorithm literature (e.g., [8, 32]). However, our definition differs in that it makes no statement about the information leaked by different query transcripts. At a high-level, a STE scheme is DO if its setup leakage \(L_S\) reveals nothing about the plaintext structure other than (potentially) the size of the structure and if its query leakage \(L_Q\) reveals nothing other than
(potentially) the size of the structure and information about the queries themselves.

**Definition 3.3** (Data-oblivious STE scheme). Let $\Sigma = (\text{Setup}, \text{Token}, \text{Query}, \text{Resolve})$ be an adaptively $(\mathcal{L}_S, \mathcal{L}_Q)$-semantically secure, response-hiding, structured encryption scheme for the data structure $\mathcal{D}_S \colon Q \rightarrow R$. We say that $\Sigma$ is data-oblivious (DO) if there exists functions $f$ and $g$ such that $\mathcal{L}_S(\mathcal{D}_S) = f(|\mathcal{D}_S|)$ and $\mathcal{L}_Q(\mathcal{D}_S, Q) = g(|\mathcal{D}_S|, Q)$.

The DO definition for interactive STE schemes is identical to Definition 3.3 except $\Sigma = (\text{Setup}, \text{Query})$. The DO property guarantees that data reconstruction attacks are impossible if the queries to $\Sigma$ are independent of the underlying data distribution (a standard assumption in the reconstruction attacks literature). This is because the information leaked by $\Sigma$ is solely a function of the size of the encrypted data structure and the queries.

### 4 ARQ: A General Framework

A primary goal of this work is to identify features of existing plaintext aggregate range query schemes that make them suitable for the encrypted setting. To do this, we introduce a general syntax for plaintext aggregate range query schemes. We then show how to derive a framework for building provably-secure, encrypted aggregate range supporting schemes from this syntax. Our framework allows us to provably characterize the leakage of any aggregate range scheme that falls within our syntax. Finally, we introduce a data independence definition that captures a set of plaintext aggregate range query schemes that may produce a provably DO scheme.

Before presenting our framework, we first define our syntax for plaintext aggregate range query schemes. All of the plaintext schemes we consider in this work (and those from Demertzis et al. [20]) fit into this syntax.

**Definition 4.1** (Aggregate range query scheme). An aggregate range query scheme $\Pi = (\mathcal{S}, \mathcal{Q}, \mathcal{R})$ for a database $\mathcal{D}_S$ consists of three polynomial-time, deterministic algorithms that work as follows:

1. $\mathcal{S}(\mathcal{D}_S)$ takes as input a database $\mathcal{D}_S$ and outputs an index structure $\mathcal{D}_S : U \rightarrow \mathcal{S}$.
2. $\mathcal{Q}(m, Q)$ takes as input the domain size $m$ and a query $Q$. It outputs a initial set of subqueries $U \subseteq U$ to be issued to $\mathcal{D}_S$.
3. $\mathcal{R}(st, R, U) \leftarrow R(st, m, Q, S)$ aggregates a set of responses from $\mathcal{D}_S$. It takes as input prior state $st$ (which may be $\perp$), the domain size $m$, the initial query $Q$, and a set of responses $S \subseteq \mathcal{S}$. It then outputs new state $st'$, an aggregate $R$ (which may be $\perp$), and a set of additional subqueries to be issued $U$ (which may be $\perp$).

We now describe $\text{ARQ}_{\Sigma, \mathcal{S}, \mathcal{Q}, \mathcal{R}}$, our framework for encrypted aggregate range query schemes. $\text{ARQ}_{\Sigma, \mathcal{S}, \mathcal{Q}, \mathcal{R}}$ is a (possibly) interactive STE scheme which is parameterized by an aggregate range query scheme $(\mathcal{S}, \mathcal{Q}, \mathcal{R})$ and a response-hiding STE scheme $\Sigma$ on data structure $\mathcal{S}(\mathcal{D}_S)$. The full $\text{ARQ}$ framework is defined in Figure 1. (For brevity, we refer to $\text{ARQ}_{\Sigma, \mathcal{S}, \mathcal{Q}, \mathcal{R}}$ as $\text{ARQ}$ in the paper when the parameters are implied from context.) In $\text{ARQ}$, the client converts their database $\mathcal{D}_S$ into an aggregate query index $\mathcal{D}_S \leftarrow \mathcal{S}(\mathcal{D}_S)$. Then, $\Sigma, \text{Setup}$ is used to encrypt $\mathcal{D}_S$. When the client performs a range query, they use $\mathcal{S}$ and $\Sigma, \text{Token}$ to determine which search tokens to send to the server. Finally, the client decrypts the responses and passes the responses to $\mathcal{R}$. $\mathcal{R}$ may output another set of subqueries to issue to the server; otherwise, $\mathcal{R}$ outputs the final aggregate to the client.

While the general form of $\text{ARQ}$ is written in the interactive STE syntax in order to support interactive plaintext schemes, we emphasize that schemes derived from $\text{ARQ}$ do not necessarily require multiple rounds of communication—in fact, most any of the $\text{ARQ}$ schemes that we derive in this work only require a single round of communication between the client and server.

**Theorem 4.2.** If $(\mathcal{S}, \mathcal{Q}, \mathcal{R})$ is an aggregate range query scheme, and $\Sigma$ is an adaptively $(\mathcal{L}_S^\Sigma, \mathcal{L}_Q^\Sigma)$-secure, response-hiding STE scheme on data structure $\mathcal{S}(\mathcal{D}_S)$, then $\text{ARQ}_{\Sigma, \mathcal{S}, \mathcal{Q}, \mathcal{R}}$ is adaptively $(\mathcal{L}_S, \mathcal{L}_Q)$-secure, where

$$
\mathcal{L}_S(\mathcal{D}_S) = \mathcal{L}_S^\Sigma(\mathcal{D}_S),
$$

and

$$
\mathcal{L}_Q(\mathcal{D}_S, Q) = (\mathcal{L}_Q^\Sigma(\mathcal{D}_S, u))_{u \in \Lambda}.
$$

Here, $\Lambda$ is the union of $U_i$’s, where $U_i$ is the instantiation of $U$ on the $i$th loop of Query$_{\mathcal{S}, \mathcal{Q}}$.

**Proof.** Let $S^\Sigma$ be the simulator guaranteed to exist by the adaptive security of $\Sigma$ and consider the $\text{ARQ}$ simulator $S$ that works as follows. Given $L_S(\mathcal{D}_S)$, $S$ simulates the encrypted index EDS by computing $EDS \leftarrow S^\Sigma(L_S(\mathcal{D}_S))$. Given $L_Q(\mathcal{D}_S, Q)$, for each $L_Q^\Sigma(\mathcal{D}_S, u)$ in $L_Q(\mathcal{D}_S, Q)$, $S$ outputs $S^\Sigma(L_Q^\Sigma(\mathcal{D}_S, u))$.

We now show that, for all PPT adversaries $A$,

$$
Pr\_break = Pr[\text{Real}_\text{ARQ}, A = 1] - Pr[\text{Ideal}_\text{ARQ}, A, S = 1]
$$
Let $\Sigma = (\text{Setup}, \text{Token}, \text{Query}, \text{Resolve})$ be a response-hiding STE scheme, $(S, Q, R)$ be an aggregate range query scheme, $S$ be a server, and $C$ be a client. Consider the interactive encrypted aggregate range query scheme $\text{ARQ}_{\Sigma,S,Q,R} = (\text{Setup}, \text{Query})$ defined as follows:

1. compute $DS \leftarrow S(DB)$;
2. compute $(K, EDS) \leftarrow \Sigma.\text{Setup}(1^k, DB)$;
3. output $(K, EDS)$;
4. $R \leftarrow \text{Query}_{\Sigma,S}(K, Q)$:
   - $C$ sets $st \leftarrow \bot$ and $R \leftarrow \bot$;
   - $C$ computes $U \leftarrow Q(m, Q)$;
   - while $U \neq \bot$,
     - (a) for all $u_i \in U$,
       - i. $C$ computes $\text{stk}_i \leftarrow \Sigma.\text{Token}(K, u_i)$;
       - ii. $C$ sends $\text{stk}_i$ to server;
     - (b) for all $\text{stk}_i$,
       - i. $S$ computes $ct_i \leftarrow \Sigma.\text{Query}(\text{stk}_i, EDS)$;
       - ii. $S$ sends $ct_i$ to client;
   - (c) initialize set $S$;
   - (d) for all $ct_i$;
     - i. $C$ computes $s_i \leftarrow \Sigma.\text{Resolve}(K, ct_i)$;
     - ii. $C$ adds $s_i$ to $S$;
   - (e) $C$ computes and sets $(st, R, U) \leftarrow R(st, Q, S)$;
4. $C$ outputs $R$

is negligible. The only difference between $\text{Real}_{\text{ARQ},A}$ and $\text{Ideal}_{\text{ARQ},A,S}$ is that all applications of $\Sigma.\text{Setup}$ and $\Sigma.\text{Token}$ have been replaced with invocations of $\Sigma$’s simulator $S^\Sigma$. Thus, in order for the adaptive semantic security of $\Sigma$ to hold, $Pr_{\text{break}}$ must be negligible.

**4.1 Data Independence**

Motivated by the security guarantees of Definition 3.3, we now identify properties of aggregate range query schemes and STE schemes that result in an instantiation of ARQ that satisfies the DO requirements. We first introduce a notion of data independence over a plaintext aggregate range query scheme. Intuitively, if $(S, Q, R)$ is data independent, then the size of all responses to queries is identical given input databases $DB$ of the same size and the subqueries generated by $Q$ and $R$ do not depend on the original table $DB$ passed to $S$.

**Definition 4.3** (Data independence). Let $(S, Q, R)$ be a plaintext aggregate range query scheme, $(DB_0, DB_1)$ be a pair of tables of size $m = |DB_0| = |DB_1|$, and $T = Q_1, \ldots, Q_s$ be a query transcript. Then, for each $Q \in T$, let $U \leftarrow Q(m, Q)$. Then, for $i \in \{0, 1\}$, let

$$DS_i \leftarrow S(DB_i),$$

$$S_{i,0} \leftarrow \{DS_i[u] \mid u \in U\}, \quad \text{and} \quad (st_{i,0}, R_{i,0}, U_{i,0}) \leftarrow R(\bot, m, Q_i, S_{i,0}).$$

Then, for $j > 0$,

$$(st_{i,j}, R_{i,j}, U_{i,j}) \leftarrow \begin{cases} R(st_{i,j-1}, m, Q_i, S_{i,j-1}) & \text{if } U_{i,j-1} \neq \bot \\ (\bot, R_{i,j-1}, \bot) & \text{if } U_{i,j-1} = \bot \end{cases}$$

We say that $(S, Q, R)$ is a data independent aggregate range query scheme if all of these conditions are true:

1. $|DS_0| = |DS_1|$ and
2. $U_{0,j} = U_{1,j}$ for all $j > 0$.

**Implications of data independence.** We first outline one interesting implication of the data independence definition that implies that any data independent scheme requires at most one round of communication.

**Corollary 4.4** (sketch). Let $\Pi$ be an interactive plaintext aggregate range query scheme. If $\Pi$ satisfies data independence, $\Pi$ may be converted into a non-interactive scheme with identical functionality.

The formalization of Corollary 4.4 is in Appendix B. The contrapositive of Corollary 4.4 provides an important insight—plaintext aggregate range query schemes that cannot be converted into a equivalent, non-interactive scheme will not satisfy data independence. As we describe later, this observation allows us to prune our search for plaintext schemes that can produce DO-satisfying, ARQ-based encrypted schemes.

From a security perspective, our notion of data independence captures a class of plaintext aggregate range query schemes that can be combined with the ARQ framework and a suitable choice of $\Sigma$ to produce a encrypted aggregate range scheme that satisfies our DO security property. Specifically, the following theorem states that, if $(S, Q, R)$ is data independent and $\Sigma$ is a DO, response-hiding STE encryption scheme over the data structure output by $S$, then $\text{ARQ}_{\Sigma, S, Q, R}$ is DO.

**Theorem 4.5.** Let $(S, Q, R)$ be a data independent aggregate range query scheme where $S$ outputs data structure $DS$ with query space $U$ and response space $S$ given some input database $DB$. Also, let $\Sigma$ be a DO, response-hiding STE scheme for data structure $DS : U \rightarrow S$. Then, the interactive STE scheme $\text{ARQ}_{\Sigma, S, Q, R}$ is DO.
Solutions to the range minimum query problem can be used to answer other types of range queries in exchange for a constant factor increase in time and space. We provide examples of such query type transformation techniques for encrypted databases in Appendix C in lieu of considering specialized structures for those types.

Definition 5.1 (Range minimum query). Given an array $A$ of $n$ numbers and indices $i$ and $j$ where $0 \leq i < j < n$, the range minimum query returns the smallest element of $A$ in the range $[i, j]$.

Previous results. Demertzis et al. [20] proposed two approaches to the RMQ problem which we refer to as DPPDG-Min1 and DPPDG-Min2. DPPDG-Min1 is built directly on top of the sparse table (ST) technique by Bender et al. [5]. Starting from every element in $A$, ST precomputes the answer for all queries whose range length is a power of 2 and stores it in an two-dimensional array $M$. This produces $O(m \log m)$ answers for each of the $m$ elements of $A$. Thus, the total space of $M$ is $O(m \log m)$. To answer a query for an interval $[i, j]$, ST accesses $M$ for the precomputed answers for the two overlapping intervals that exactly cover $[i, j]$. It then returns the minimum of those two answers.

DPPDG-Min1-encrypts the array generated by ST to achieve $O(m \log m)$ space with constant-size and time queries. DPPDG-Min2 is similar to DPPDG-Min1, but reduces the overhead on sparse databases to $O(m + n \log n)$ in exchange for an additional round of communication. It does this by first accessing an additional encrypted index that maps query domain values to the identifier of the record nearest to that domain value. This allows the ST to be built over the record identifiers, resulting in smaller storage when $n < m$.

It can be easily shown that DPPDG-Min1 is DO. However, DPPDG-Min2 is not DO—the scheme used by DPPDG-Min2 is interactive (and cannot be easily changed into a non-interactive scheme) and is thus not data independent as implied by Corollary 4.4.

Existing plaintext structures. Several $O(m)$-space solutions to for range minimums exist in the data management literature. However, achieving this storage bound appears to necessitate the use of various compaction techniques that make them unsuitable for our security goals. For example, some schemes [18, 22] use bit-packing techniques that condense $O(m \log m)$ bits to $O(m)$ words through the combination of different components of the structure into the same word. While these structures, in theory, could be implemented in the STE setting, practical symmetric encryption algorithms’ use...
of padding would prevent the use of bit-packing and thus $O(m \log m)$ space would be required.

Similarly, other schemes [4, 5, 28] use a related lookup table technique. At a high-level, this class of techniques saves space by storing the answers to all possible queries in a compact lookup table. Then, queries to the structure return a reference to a part of the lookup table, which must be separately queried to retrieve the actual answer. These kinds of structures are also unsuitable for our DO security goals for the following reasons: first, Corollary 4.4 implies the multi-round nature of the lookup table technique makes it impossible for the plaintext scheme to be data independent, and thus the resulting ARQ scheme will not be DO. More specifically, if two queries to the structure require the user to query the same component of the lookup table, then the access pattern leakage on the lookup table reveals that both queries had the same answer. Thus, the access pattern leakage on the lookup table can change when the contents of the underlying database changes, which would make the resulting ARQ scheme not DO.

5.1 Our Approach

Modified Fischer-Heun (FH) algorithm. In light of the aforementioned concerns, we describe how to adapt the scheme of Fischer and Heun [28] in such a way that the resulting plaintext scheme satisfies the constraints given by Corollary 4.4 and maintains the $O(m)$ space and $O(1)$ query time requirements in exchange for the restriction that clients are not allowed to issue range queries with length that is less than some small size $s$. Our modifications result in a DO scheme.

We first present a slightly simplified version of FH which will be suitable for the description of our encrypted approach. FH works by first partitioning the table DB into blocks $B_1, \ldots, B_{m/s}$ of size $s = \log m$. Then, an array $A$ of size $m/s = m/\log m = O(m)$ is generated, where $A[i] = \langle \min(B_i), \text{indexof}(DB, \min(B_i)) \rangle$. The ST technique is then applied over $A$ to produce the sparse table $M$ of size $O(\frac{m}{\log m} \log \frac{m}{\log m}) = O(m)$. Finally, a normalization technique is applied to generate a lookup table of size $O(m)$ that stores the answers to all possible queries on arrays of size $s$. (We elide the details of this part of the scheme, since it does not affect our approach.) Queries are answered by taking the minimum of the minima for the following three ranges:

Let $\text{SparseTable}(A)$ denote an application of the ST algorithm [5] on array $A$. Consider the aggregate range query scheme $\Pi^{\text{LinearMin}} = (S, Q, R)$ defined as follows:

- **DS $\leftarrow S(DB)$**:
  1. Initialize arrays $A$, $L_{\text{left}}$, and $L_{\text{right}}$;
  2. compute $s = \log m/4$;
  3. partition DB into blocks $B_1, \ldots, B_{m/s}$ of size $s$;
  4. for $i \in [m/s]$, set $A[i] := \min(B_i)$;
  5. compute $M \leftarrow \text{SparseTable}(A)$;
  6. for $i \in [m]$,
     
     - (a) compute block index $b$ of index $i$;
     - (b) set $L_{\text{left}}[i] := \min_{b \leq k \leq s} DB[k]$;
     - (c) set $L_{\text{right}}[i] := \min_{b + 1 \leq k \leq (b+1)-1} DB[k]$;
  7. output $\text{DS} \leftarrow (M, L_{\text{left}}, L_{\text{right}})$;

- **U $\leftarrow Q(m, Q)$**:
  1. parse $(\ell, r) \leftarrow Q$;
  2. if $r - \ell < s$, abort;
  3. compute $b_\ell \leftarrow \lfloor \frac{\ell}{s} \rfloor$ and $b_r \leftarrow \lfloor \frac{r}{s} \rfloor$;
  4. set $q_1 \leftarrow \ell$ and $q_2 \leftarrow r$;
  5. if $b_r - b_\ell > 1$,
     - (a) compute $h \leftarrow \lceil \log(b_r - b_\ell + 1) \rceil$;
     - (b) compute $q_3 \leftarrow (b_h, h)$ and $q_4 \leftarrow (b_r - 2^h + 1, h)$;
     - (c) output $(q_1, q_2, q_3, q_4)$;
  6. else, output $U \leftarrow (q_1, q_2)$;

- $(\text{st}', R, U) \leftarrow R(\text{st}, m, Q, S)$;
  1. output $(\bot, \min(S), \bot)$.

![Fig. 2. The plaintext $\Pi^{\text{LinearMin}}$ scheme used to instantiate the encrypted $\Pi^{\text{LinearMin}}$ scheme.](image)

1. From $\ell$ to the end of $\ell$’s block using the normalization table to find the index of the minimum, then using $A$ to retrieve the actual minimum.
2. The range spanning all blocks between $\ell$’s block and $r$’s block using $M$ (does not require accessing $A$).
3. From the start of $r$’s block to $r$ using the normalization table, then using $A$ for the actual minimum.

However, directly transforming the FH scheme into an STE structure results in problematic leakage from the lookup table invoked in subproblems 1 and 3.

Thus, we now introduce $\Pi^{\text{LinearMin}}$, our modified FH scheme. Figure 2 outlines the algorithm for the scheme, and Figure 3 provides an example of the scheme. Our scheme is exactly the same as in the FH algorithm except with the following modifications. First, the user is prevented from making some queries that are smaller than $s$—in particular, those queries that lie entirely within a block $B_i$. (For example, a database of size $m = 2^{64}$ has block size $s = \log 2^{64} = 64$, and so some queries of size smaller than 64 are not permissible.) This allows us to avoid using the lookup tables from the original FH scheme. However, with a simple
modification, we can still answer arbitrary queries of size at least \( s \). To do this, we create two arrays \( L_{\text{left}} \) and \( L_{\text{right}} \) of size \( m \) which we use to precompute one-sided queries within each block \( B_i \). Specifically, given index \( i \) in block index \( b \), we assign \( L_{\text{left}}[i] := \min_{s \leq k \leq 1} \left( \text{DB}[k] \right) \) and \( L_{\text{right}}[i] := \min_{s \leq k \leq |B_i| - 1} \left( \text{DB}[k] \right) \). We can then answer a query \( [l, r] \) by retrieving the answers for at most three of the following subproblems:

1. From \( \ell \) to the end of \( \ell \)'s block using \( L_{\text{right}} \).
2. The range spanning all blocks between \( \ell \)'s block and \( r \)'s block using \( M \).
3. From the beginning of \( r \)'s block to \( r \) using \( L_{\text{left}} \).

Since any query of size \( s \) or greater must touch or overlap at least one block boundary, we may answer any such query using the structures above. Thus, all queries are answerable in constant time. Queries that are smaller than size \( s \) also may be answered provided that they touch or overlap at least one block boundary.

**LinearMin:** A New Linear-Space Scheme. Combination of \( \Pi_{\text{LinearMin}} = (S, Q, R) \) with the ARQ framework results in a provably secure scheme, \( \text{LinearMin} = \text{ARQ}_{\Sigma, S, Q, R} \), for the encrypted range minimum problem with the leakage profile given in Theorem 4.2.

**Lemma 5.2.** \( \Pi_{\text{LinearMin}} \) is data independent.

**Proof (sketch).** Given any pair of databases \((\text{DB}_0, \text{DB}_1)\), \( S \) always outputs \( M \), \( L_{\text{left}} \), and \( L_{\text{right}} \) with the same respective size regardless of whether or not \( \text{DB}_0 \) or \( \text{DB}_1 \) is chosen. Thus, \(|S| = |S_0| = |S_1|\). Additionally, given a query \( Q \), \( Q \) always outputs the same set of subqueries \( U_0 \) for \( Q \) (as it is deterministic and has no knowledge of the underlying DB). This implies that the size of the initial subresponse set \( S_0 \) is identical for both databases. Also, \( \mathbb{R} \) always outputs \( \perp \) for \( U_j \) for \( j > 0 \), so we know that \( U_{0,j} = U_{1,j} \) for all \( j > 0 \).

**Theorem 5.3.** Given \( \Pi_{\text{LinearMin}} = (S, Q, R) \) and a response-hiding STE scheme \( \Sigma \) on data structure \( DS \) with storage space \( O(|DS|) \) and constant query time and space, the scheme \( \text{LinearMin} = \text{ARQ}_{\Sigma, S, Q, R} \) is DO, supports queries on ranges of size at least \( \log m \), and requires \( O(m) \) storage, \( O(1) \) query time at both the client and server, and \( O(1) \) bandwidth.

Theorem 5.3 follows by Lemma 5.2 and from [28].

**Workarounds for query size limitation.** One simple solution to minimize the number of queries of size \( s \) that are blocked by the scheme is to recursively apply the scheme again within blocks of size \( s \). This maintains the asymptotics of the construction (at the expense of a larger coefficient on the storage overhead) and decreases the threshold where certain queries cannot be answered from \( s = \log m \) to \( s' = \log \log m \).

Additionally, in practical deployments, the encrypted minimum structure may be stored alongside an record-reporting encrypted range structure (e.g., [20, 25, 27]). In such settings, the client may use a split execution strategy [62] where, when faced with an unanswerable query, the client can send a range query to the encrypted range structure. Then, the client can compute the minimum by decrypting the returned records client-side and taking the minimum of the query attribute. Given that this is required only for some small queries (of size less than \( s \)), the client still may enjoy the performance and leakage benefits of the LinearMin scheme on larger queries while incurring minimal performance overhead for the small queries.

## 6 Range Mode Query

In this section, we propose a novel scheme for the encrypted approximate range mode query problem, which asks for the element with the maximum number of occurrences in a given range of an array. The current state-of-the-art storage bound for constant-time range mode queries over static arrays is \( O(n^2 \log \log n / \log^2 n) \) [59]. Given this near-quadratic storage requirement, we instead consider an approximate version of the range mode query problem. Similar approximations are available in several database implementations to improve performance (e.g., the APPROXIMATE_MEDIAN and APPROXIMATE_MODE functions in Vertica [63]). Intro-
duced by Bose et al. [12], the approximate range mode query problem asks us to return an element of the queried range whose frequency is at least \( 0 < \alpha < 1 \) times that of the frequency of the actual mode of \( A' \).

**Definition 6.1 (\( \alpha \)-approximate mode query).** Given an array \( A \) of size \( n \) and indices \( i \) and \( j \) where \( 0 \leq i \leq j < n \), let \( A' \) be the multiset of elements comprised of all elements of \( A \) between the indices \( i \) and \( j \) (inclusive). We say that an element \( x \in A' \) is an \( \alpha \)-approximate mode of \( A' \) if \( \text{freq}(x, [i, j]) \geq \alpha \cdot \text{freq}(x, [i, j]) \) where \( \text{freq}(x, [i, j]) \) returns the frequency of \( x \) in the range \([i, j]\) and \( 0 < \alpha < 1 \). The \( \alpha \)-approximate range mode query returns an \( \alpha \)-approximate mode of \( A' \).

Observe that the accuracy of the approximation increases as \( \alpha \) tends to 1.

**Other existing plaintext structures.** Several solutions have been proposed that solve the approximate range mode problem with varying degrees of efficiency. Many of these schemes use bit-packing techniques that, as explained previously, we can not directly translate to STE structures (e.g., [33, 52]) or rely on theoretical data structures with no practical implementation (e.g., [23]). Additionally, while some recent schemes achieve lower storage requirements than our chosen approach, their query algorithms require non-constant query time (e.g., [23]). In all such cases, queries required at least 2 round trips to the structure and subsequent accesses to the query structure depended on the result of the initial access. These features meant that the schemes would not be data independent as changes to the underlying database would result in different access patterns; additionally, as shown by Corollary 4.4, the interactivity of the scheme makes the schemes non-data-independent.

### 6.1 Our Approach

**The BKMT scheme.** Given the above constraints, we focus our attention on the structures developed by Bose, Kranakis, Morin, and Tang (BKMT) [12]. The BKMT scheme relies on the following technical theorem.

**Theorem 6.2 (Mode partition [12]).** If \( \{B_1, \ldots, B_k\} \) is a \( k \)-partition of the range \([\ell, r]\), then \( \arg \max_x \text{mode}(B_p) \geq \frac{\text{mode}(\ell, r)}{k} \), where mode is the function that returns the mode of the input range on \( A \). Then, of the \( k \) submodes \( \text{mode}(B_1), \ldots, \text{mode}(B_k) \), the submode with the highest frequency is an \( 1/k \)-approximate mode of \([\ell, r]\).

Consider the aggregate range query scheme \( P_{1/2-\text{ApproxMode}} = (S, Q, R) \) defined as follows:

1. compute \( k \leftarrow \left\lceil \log m \right\rceil \);
2. for \( p \in [0, k) \),
   a. for \( h \in [0, \lfloor m/2^p \rfloor] \),
      i. compute \( s \leftarrow h \cdot 2^p \);
      ii. compute \( h \leftarrow \min(s + 2^{p-1}, m) \);
   b. for \( 1 \leq i \leq h \), compute the \((\text{mode}, \text{freq})\) pair for the range \([1, i]\) and set in \( M([p, i]) \);
3. output \( DS \leftarrow M \);
4. compute \( (R, f) \leftarrow \arg \max_{x,f} \in S \{f\} \);
5. output \( (\bot, R, \bot) \);

---

Yao [66] and Alon and Schieber [2] provide the necessary \( k \)-partitioning scheme for Theorem 6.2. We refer to this technique as the AS technique. AS is similar to the previously mentioned ST technique except that, in AS, the \( k \)-intervals in a given partition do not overlap. Here, we describe the AS partitioning algorithm for the case when \( k = 2 \). For \( k = 2 \), AS splits the array at point \( h = 2^{\lfloor \log m \rfloor} \) into two blocks. Then, for \( 1 \leq i \leq h \), AS precomputes the answers to all intervals \([i, h]\). Similarly, for \( h + 1 \leq j \leq m \), AS precomputes the answers to all intervals \([h+1, j]\). These intervals allow us to answer any query \([\ell, r]\) that intersects the halfway point \( h \). To answer queries that fall entirely within one half of the array (i.e., where \( r \leq h \) or \( \ell \leq h + 1 \)), AS recursively processes each half of the array with the same algorithm. Each level of the resulting table represents \( m \) intervals computed at one of the \( O(\log m) \) recursive steps.

The BKMT solution follows as a combination of Theorem 6.2 and the AS technique. At setup time, we generate a \( k \)-interval AS table \( M \) that stores the mode of each interval and the mode’s frequency. Then, to answer a query \([\ell, r]\), we query the \( k \) non-overlapping intervals in \( M \) that exactly cover \([\ell, r]\) to retrieve their modes. By Theorem 6.2, the mode with the highest frequency of all \( k \) modes is a \( 1/k \)-approximate mode of \([\ell, r]\). This scheme is described in Figure 4.

---

**Fig. 4.** The plaintext \( P_{1/2-\text{ApproxMode}} \) scheme used to instantiate the encrypted \( 1/2-\text{ApproxMode} \) scheme.
1/2-APPROXMODE: A New Encrypted Mode Scheme. Combination of \( \Pi_{1/2-\text{APPROXMODE}} = (S, Q, \mathcal{R}) \) with the ARQ framework results in a provably secure scheme, 1/2-APPROXMODE = ARQ\(S, S, Q, \mathcal{R}\), for the encrypted range mode problem with the leakage profile given in Theorem 4.2.

**Lemma 6.3.** \( \Pi_{1/2-\text{APPROXMODE}} \) is data independent.

Lemma 6.3 can be proved similarly to Lemma 5.2.

**Theorem 6.4.** Given \( \Pi_{1/2-\text{APPROXMODE}} = (S, Q, \mathcal{R}) \) and a response-hiding STE scheme \( \Sigma \) on data structure DS with storage space \( O(|DS|) \) and constant query time and space, the scheme 1/2-APPROXMODE = ARQ\(S, S, Q, \mathcal{R}\) is DO and requires \( O(m \log m) \) storage, \( O(1) \) query time at both the client and server, and \( O(1) \) bandwidth.

Theorem 6.4 follows by Lemma 6.3 and from [12].

1/3-APPROXMODE. 1/3-APPROXMODE, a scheme for answering encrypted 1/3-range mode queries, is equivalent to 1/2-APPROXMODE except we modify \( \Pi_{1/2-\text{APPROXMODE}} \) to use a 3-interval AS table. Queries then involve three intervals instead of two. This improves the storage requirement to \( O(m \log \log m) \) in exchange for a wider approximation. We omit the full description of this approach and direct the reader to [2] for the \( k \)-interval partition algorithm for \( k > 2 \).

**7 Range Median Query**

In this section, we propose a novel encrypted scheme for the encrypted approximate range median query problem. Like the range mode problem, the exact range median query problem has near-quadratic storage overhead for constant-time queries, with the best known solution requiring \( O(n^2 \log^k n) \) storage, where \( k \) is an arbitrary constant and \( \log^k \) is the iterated logarithm function [58]. We thus concentrate on solutions for the approximate version of the problem introduced by Bose et al. [12]. Given \( 0 < \alpha < 1 \), the \( \alpha \)-approximate median query asks for an element of the queried range whose rank is within \( \pm \alpha/2 \) of the rank of the true median.

**Definition 7.1** (Approximate median query). Given an array \( A \) of \( n \) numbers and indices \( i \) and \( j \) where \( 0 \leq i \leq j < n \), let \( A' \) be the multiset of elements comprised of all elements of \( A \) between the indices \( i \) and \( j \) (inclusive). Given \( 0 < \alpha < 1 \), we say that an element \( x \in A' \) is an \( \alpha \)-approximate median of \( A' \) if the percentile rank of \( x \) in \( A' \), denoted \( r_x \), satisfies \( r_x \in \left[ \frac{1}{2} - \frac{\alpha}{2}, \frac{1}{2} + \frac{\alpha}{2} \right] \). The \( \alpha \)-approximate range median query returns an \( \alpha \)-approximate median of \( A' \).

Note that in the above definition, the accuracy of the approximation increases as \( \alpha \) tends to 1.

**Other existing plaintext structures.** We know of one other constant time and bandwidth approximate median scheme [23]. It uses fusion trees, a theoretical data structure with no practical implementation, so we do not consider it in this work.

**7.1 Our Approach**

**A modified version of the BKMT scheme.** We use a scheme based on the \( \alpha \)-approximate range median index from Bose, Kranakis, Morin, and Tang (BKMT) [12]. In our testing, we found that the original BKMT query algorithm sometimes produced queries to indices that were outside the bounds of the structure; this was the case whether or not the domain size matched the paper’s assumption that it was a strict power of two. However, we found that the setup algorithm from BKMT was correct. The scheme we present here is identical to the BKMT scheme with a modified query algorithm that fixes the out-of-bounds issues but preserves the constant time and size query overhead.

We refer to our modified scheme as \( \Pi_{\alpha-\text{APPROXMEDIAN}} \). Figure 6 defines the scheme and Figure 7 illustrates an example. The algorithm relies on the following observation: given a sufficiently long query interval, the effects of the elements in a small prefix and suffix of the interval are minimal on the median and thus can be
Let $\text{BKMTApproxMedian}(\alpha, \DB)$ denote an application of the BKMT $\alpha$-approximate median algorithm over table DB [5]. Consider the aggregate range query scheme $\Pi_{\alpha, \text{APPROXMEDIAN}} = (\Sigma, \Q, \R)$ defined as follows:

1. $\text{DS} \leftarrow \Sigma(\DB)$:
   - 1. Initialize dictionary $\DX$;
   - 2. Compute $k \leftarrow \lceil \log m \rceil$ and $p \leftarrow \lfloor \frac{2(1+\alpha)}{1-\alpha} \rfloor$;
   - 3. For $1 \leq i \leq k$,
     - (a) Compute $b \leftarrow 2^{k-i}$;
     - (b) For $1 \leq j \leq \lfloor \frac{p}{2} \rfloor$,
       - i. Initialize list medians;
       - ii. For $1 \leq x \leq p$,
         - A. Compute $s \leftarrow \min((j-1) \cdot b, m-1)$;
         - B. Compute $e \leftarrow \min(s + (x \cdot b), m)$;
         - C. Compute the median from $s$ to $e$ in $\DB$ and append it to medians;
     - iii. Set $\DX[(i, j)] := \text{medians}$;
   - 4. Output $\text{DS} \leftarrow (\DX)$;

2. $U \leftarrow \Q(m, \Q)$:
   - 1. Parse $(\ell, r) \rightarrow x$;
   - 2. Compute $\text{max}\_\text{blocks} \leftarrow 2 \cdot \lfloor \frac{2\alpha}{1-\alpha} \rfloor$;
   - 3. Compute $k \leftarrow \lceil \log m \rceil$;
   - 4. Compute $\text{initial}\_\text{level} \leftarrow k - \lfloor \log(r - \ell) \rfloor + 1$;
   - 5. Compute $\text{offset} \leftarrow \lfloor \log(\text{max}\_\text{blocks} + 2) \rfloor - 2$;
   - 6. Compute $i \leftarrow \min(\text{initial}\_\text{level} + \text{offset}, k)$;
   - 7. Compute $b \leftarrow 2^{k-i}$;
   - 8. Compute $b_l \leftarrow \lceil \frac{k}{b} \rceil + 1$ and $b_r \leftarrow \lfloor \frac{k}{b} \rfloor$;
   - 9. Output $U \leftarrow ((i, b_l), b_r)$;

3. $(\ell', R, U') \leftarrow R(\ell, m, \Q, S)$:
   - 1. Recompute $b_l$ and $b_r$ using $\Q$;
   - 2. Compute $x \leftarrow b_r - b_l$;
   - 3. Output $(\ell', S[x], \perp)$;

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig6}
\caption{The plaintext $\Pi_{\alpha, \text{APPROXMEDIAN}}$ scheme used to instantiate the encrypted $\alpha$-APPROXMEDIAN scheme.}
\end{figure}

Theorem 7.3 follows by Lemma 7.2 and from [12].

Lemma 7.2. $\Pi_{\alpha, \text{APPROXMEDIAN}}$ is data independent.

Lemma 7.2 can be proved similarly to Lemma 5.2.

\begin{proof}
Given a table $\DB$ with domain size $m = 2^k$ for some $k \geq 1$, BKMT creates a hierarchical set of arrays $T_1, \ldots, T_k$ as follows. For $1 \leq i \leq k$, we partition $\DB$ into $2^i$ blocks of size $m/2^i$. Then, $T_i$ contains $2^i$ entries $T_i[j]$, each of which corresponds to the $j$th block of size $m/2^i$, denoted $B_{i,j}$. Then, each $T_i[j]$ is a list containing $p = \lfloor \frac{2(1+\alpha)}{1-\alpha} \rfloor$ elements of $\DB$, where, for all $1 \leq i \leq p$,

\[ T_i[j][x] := \text{median}(\bigcup_{0 \leq q < x-1} B_{i,(j+q)}) \]

Each array $T_i$ contains $2^i$ lists, each containing $\lfloor \frac{2(1+\alpha)}{1-\alpha} \rfloor$ elements. Thus, each $T_i$ is of size $O(\frac{2(1+\alpha)}{1-\alpha})$. There are $\log m$ arrays, so the total space needed to store them is $\sum_{i=1}^{\log m} O(\frac{2(1+\alpha)}{1-\alpha}) = O(m(1+\alpha)) = O\left(\frac{m}{1-\alpha}\right)$. Answering a query $[\ell, r]$ can be done in $O(1)$ by accessing a single element in $T$ using the following algorithm:

1. Determine which $T_i$ was generated from blocks that are as large as possible but still fit within the query length $r - \ell$ (lines 2 through 6 in Figure 7).
2. Given the block size $b \leftarrow 2^{k-i}$ used to generate $T_i$, compute block indices of $\ell$ and $r$ as $b_\ell = \lceil \frac{k}{b} \rceil + 1$ and $b_r = \lfloor \frac{k}{b} \rfloor$.
3. Output $T_i[b_\ell][b_r - b_\ell] = \text{median}(\bigcup_{0 \leq q < b_r} B_{i,(b_\ell+q)})$.

\end{proof}

8 Exploiting Sparsity

We now present a set of storage optimizations for encrypted aggregate range query structures over sparse databases. We refer to our techniques as domain reductions, as they allow the client to reduce the size of the domain that the aggregate structure is built over. Our reductions themselves are plaintext aggregate range query schemes that convert the query space of an encrypted data structure to a smaller domain space, while still allowing the client to make queries in the original domain that the aggregate structure is built over.
Let \( \Pi' = (S', \mathcal{Q}', R') \) be a plaintext aggregate range query scheme. Consider the aggregate range query scheme \( \Pi_{DomainBucket}(S', \mathcal{Q}', R') = (S, \mathcal{Q}, R) \) defined as follows:

1. Initialize multimap \( MM \);
2. for all \( 0 \leq i \leq m^{1-\alpha} \),
   (a) compute \( \ell \leftarrow im^\alpha \) and \( r \leftarrow ((i+1)m^\alpha) - 1 \);
   (b) compute \( L_1 \leftarrow \text{DB}^{-1}(\ell - 1) \) and \( L_2 \leftarrow \text{DB}^{-1}(r + 1) \);
   (c) compute bucket, \( \leftrightarrow \{ (j, DB(j)) \mid j \in [\ell, r] \} \cup \{L_1, L_2\} \);
   (d) set \( \text{MM}[\ell, r] := \text{bucket} \);
3. compute \( DS' \leftarrow S'(\text{DB}) \);
4. output \( DS \leftarrow (\text{MM}, DS') \);

query space. In general, our reductions enable the client to efficiently find the ID of the record whose query attribute is closest to the client’s desired query. Our reductions significantly reduce storage with different trade-offs between query performance and leakage.

Our domain reduction schemes are presented in terms of the plaintext aggregate range query syntax from Definition 4.1, though the reductions themselves are parameterized by a secondary scheme. Defining our reductions in this way allows us to immediately apply the ARQ framework to our reductions to derive encrypted aggregate range query schemes.

The DomainBucket reduction. Figure 9 illustrates the DomainBucket reduction; the algorithm is defined in Figure 8. The reduction takes as input the domain size \( m \), the database DB, and a tunable constant \( 0 < \alpha < 1 \). We partition the domain of DB into non-overlapping “buckets” where each bucket has equal size. More precisely, we instantiate a multimap \( MM \) with keys \( \{[im^\alpha, (i+1)m^\alpha) - 1] \mid i \in [m^{1-\alpha}] \} \), where the \( i \)th label holds tuples corresponding to the all of the records in the range \([im^\alpha, (i+1)m^\alpha) - 1] \). Each tuple has two elements: the original domain value and the ordered ID of the record (i.e., the transformed domain).

We also store two additional entries in each bucket that we call “backwards/forwards lookup” entries. The first entry corresponds to the record that is closest to the left endpoint of the bucket, but is not within the bucket range itself; the second record is for the right endpoint of the bucket. This allows the client to receive a valid answer to a query even if their original query falls in a bucket with no records.

When making a query to the structure, the client sends a search token corresponding to the bucket containing the domain point. The server responds with the entire bucket. The client then does a linear pass to find the record ID of the closest element to \( x \).

Complexity of DomainBucket. DomainBucket requires only a constant-size search token corresponding to the desired bucket range of size \( m^\alpha \). However, the response bandwidth from the server to the client is potentially linear—consider a database where all of the records are in a single bucket range, and thus a query to that range will return \( O(n) \) records. Thus, the worst-case client computation complexity is \( O(n) \), as such a database would require the client to sort through all \( O(n) \) records to recover the nearest populated point.

The DataBucket reduction. The volume leakage and the worst-case-linear bandwidth of the DomainBucket scheme motivates our second domain reduction con-
To ensure that their volumes are indistinguishable. This allows for future queries. Buckets are padded with \( \perp \) to ensure that their volumes are indistinguishable. This brings the bandwidth in the worst case from \( O(m^a) \) to \( O(m^a) \) (i.e. the maximum size of a bucket).

**Example: range sum queries.** With our domain reduction schemes in hand, we use this section as an example of how our domain reductions can be used to derive optimizations to the encrypted range sum scheme presented by Demertzis et al. [20], which require \( O(m) \) storage.

**Definition 8.1 (Range sum query).** Given an array \( A \) of \( n \) numbers and indices \( i \) and \( j \) where \( 0 \leq i \leq j < n \), the range sum query computes \( \sum_{k=i}^{j} A[k] \), the sum of all \( A[k] \) where \( i \leq k \leq j \).

Solutions to the range sum query problem can be used to answer **count**, **average**, and **variance** queries in exchange for a constant factor increase in time and space. We provide examples of such **query type transformation** techniques for encrypted databases in Appendix C in lieu of considering specialized structures for those types.

**Previous results.** Demertzis et al. [20] presented the first and only encrypted range sum query STE scheme, DPPDG-SSum, which was based on the classic **prefix sums** technique [9]. This technique allows for constant-size and constant-time queries in exchange for \( O(m) \) storage. In this technique, an array \( A \) of size \( m \) is computed such that, for all \( x \in [m] \), \( A[x] := \sum_{i=0}^{x} DB(x) \).

Then, a range sum query \([\ell, r]\) may be answered in constant time by accessing \( A[r] \) and \( A[\ell-1] \), then computing

\[
A[r] - A[\ell-1] = \sum_{i=0}^{r} DB(x) - \sum_{i=0}^{\ell-2} DB(x) = \sum_{i=\ell-1}^{r} DB(x).
\]

The DPPDG-Sum scheme translates prefix sums to the encrypted range sum problem by encrypting \( A \) with an array encryption scheme. (We note that ARQ can be used to derive this scheme and its leakage.)

**Our derived schemes.** Our reductions may be compiled directly on top of DPPDG-Sum to reveal the asymptotics detailed in Table 1. To do this, we generate the prefix sums array \( A \) over the \( n \) sorted record IDs in \( \text{DB} \) as the domain values. (Observe that the “domain” of this prefix sums array is over the \( O(n) \) record IDs of \( \text{DB} \).) Then, we apply our choice of reduction to the array \( A \). When the client wants to make a query \([\ell, r]\), they make two queries to the reduction structure—one to find the nearest record ID \( \text{id}_r \) on the left of \( \ell \), and another to find the nearest record ID \( \text{id}_r \) on the right of \( r \). The client then queries \( A \) using \([\text{id}_r, \text{id}_r] \).

Under our general domain reduction framework, the added structure normally incurs an additional round of communication. However, for prefix sums, we may avoid the additional round of communication due to the following: since every record ID has a one-to-one mapping with an entry in the prefix sums array, we can replace every instance of the record ID in the domain reduction structure with its entry in the prefix sums array. Now, when the client makes a query to the domain reduction structure, the structure’s response is the desired sum.

**Tradeoffs and potential attacks.** While our reductions result in substantially lower storage overhead on sparse datasets, the leakage changes result in schemes that are not provably DO. However, the lack of the DO property does not mean that the schemes are immediately vulnerable to attacks. To provide more context on this trade-off, we now describe starting points for attacks against the domain reductions and what assumptions may be necessary for such attacks to produce practical impact.

Consider some instantiation of \( \text{ARQ}_{\Sigma, S, Q, R} \) where \((S, Q, R)\) is derived from a domain reduction scheme. Given that the reduction index translates coordinates in the original query space \( Q^* \) into a new query space \( Q \) and, generally, \(|Q^*| < |Q|\), at least two queries to the domain reduction index will be transformed into the same query to the aggregate index structure. In the specific reductions we propose in this work, this duplication may reveal information about the density distribution of the underlying database.
9 Empirical Evaluation

We now evaluate how the schemes derived from the ARQ framework perform in practice.

Arca: a new structured encryption library. As part of this work, we designed and implemented a new, open-source, encrypted search library called Arca [24]. (Arca’s code is available at https://github.com/cloudsecuritygroup/arca.) Arca is a Python package designed to allow researchers to easily and rapidly prototype systems that use encrypted search algorithms. It provides simple cryptographic primitives (which themselves are based on those provided by the Python cryptography package [61]) and implementations of various structured encryption schemes. Arca v0.1.0 consists of 1558 lines of code (excluding 1121 lines of tests) as counted by CLOC v1.92 [1]. Arca has complete type annotations and passes all strict type checks provided by MyPy.

We implemented all of the plaintext schemes that we chose in this work as well as the plaintext schemes used by Demertzis et al. [20]. Then, using Arca, we implemented the ARQ framework. Combining our implementation of the ARQ framework and our implementations of the plaintext schemes produced the LinearMin, 1/2-ApproxMode, α-ApproxMedian, DomainBucket, and DataBucket encrypted schemes as well as the encrypted schemes from [20]. The plaintext implementations of these schemes and the ARQ framework are included within the Arca 0.1 library.

Cryptographic primitives. We used the cryptographic primitives provided by Arca. For symmetric encryption, we used AES-256 in CBC mode; for PRFs, we used SHA512. For each ARQ instantiation, we used Arca’s implementation of the Πbias scheme from [14] as Σ.

Experimental setup. We ran our experiments single-threaded on a Slurm computing cluster consisting of Intel Xeon E5-2670 and E5-2600 processors. All experiments were performed in-memory, with each process allotted 300 GB of RAM. (Our experiment code is at https://github.com/cloudsecuritygroup/arq-experiments.)

Datasets. We use two real-world datasets in our evaluation. Gowalla [16] was a location-based social networking website in which users could share their locations. This dataset contains a total of 6,442,892 check-ins collected from users between February 2009 and October 2010, with 5,561,630 unique records. The date and time of the check-ins were converted to Unix time integers, then shifted to domain \{0, \ldots, 54083068\}. These normalized times were used as the query attribute. Using Gowalla, we demonstrate the effects of increasing the number of records on the scheme costs by randomly partitioning Gowalla into 12 sets of 500,000 points. We ran our schemes on one partition, then formed a new dataset by adding another partition to the previous partitions and benchmarked the costs again with the increased number of records.\(^1\) We use this dataset (and this partitioning scheme) to replicate Demertzis et al.’s [20] evaluation of their schemes.

Amazon [54] contains 51,311,621 item ratings from reviews left in the Books section of Amazon between May 1996 and October 2018. There are 7,837 unique timestamps in the dataset. We normalized the timestamp of the reviews to the domain \{0, \ldots, 7058880\}. Quantitative evaluation. Figure 11 demonstrates the effectiveness of our domain reductions in reducing the index size, construction time, and server query time of

---

\(^1\) We were unable to run the DPPDGP-Min1 scheme on any partition set of Gowalla within 8 hours due to the number of encryptions needed to encrypt the ST. Thus, we instead computed the number of bytes needed to store the encrypted form of each entry of ST (162 B) and the average time for computing a hash of each entry’s label and encrypting its value (15356 ns). Then, we computed the \# of cells in the ST and extrapolated the index size and runtime of DPPDGP-Min1 using the previous two metrics. Note that our encryption time estimate is conservative, as it does not take into account the time it takes to access elements from the large (plaintext) ST array.
DPPDGP-Sum, while only slightly increasing the resolve time at the client. In particular, the DataBucket scheme results in significantly lower storage and construction overhead than DomainBucket—since m and α are public parameters and each bucket is the same size, the entire bucket may be encrypted as a single value which substantially reduces the amount of extra padding incurred by each encryption operation. The client-side performance tradeoffs with the reductions are made evident in the results for Resolve, but the runtime is minimally greater than that of DPPDGP-Sum.

For the minimum schemes, Figure 12 demonstrates that our LinearMin scheme (designed for dense databases) performs significantly better than DPPDGP-Min1 (its direct dense scheme competitor) and better than DPPDGP-Min2 (the scheme designed for “sparse” databases) starting at 2.5 million records in Gowalla. For the approximate schemes, Table 2 and Table 3 in the Appendix provide baseline performance benchmarks for the 1/2-ApproxMode and α-ApproxMedian schemes for α = 0.5. We can see that the storage and build time overhead of both schemes is comparable to that of DPPDGP-Min1.

In Figure 13, we plot the index size of our DomainBucket and DataBucket schemes under synthetic databases of different densities, with uniformly distributed data. We observe that the index size increases as the sparsity decreases, as expected in both cases. Due to the data distribution, we observe similar performance from the DomainBucket and DataBucket schemes.

All in all, our experiments and analysis demonstrate that our approach’s theoretical constant-size and time query overhead is very small in practice. In particular, the overhead will be significantly smaller than the linear-time overhead of the strategies used in prior work mentioned in Section 2.

Acknowledgements

Work supported in part by the National Science Foundation, the NetApp University Research Fund, and the Randy Pausch Undergraduate Summer Research Award at Brown University. Part of this research was conducted using computational resources of the Center for Computation and Visualization at Brown University.
References


A Adaptive Semantic Security

Definition A.1 (Adaptive semantic security [15]).

Let $\Sigma = (\text{Setup}, \text{Token}, \text{Query}, \text{Resolve})$ be a response-hiding structured encryption scheme for the data structure $DS : Q \rightarrow R$. Also, let $A$ be a stateful adversary, $S$ be a simulator, $L_S$ and $L_Q$ be leakage functions, and $z \in \{0,1\}^*$. Given the following probabilistic experiments:

**Real$_{\Sigma,A}(k)$:** Given $z$, $A$ outputs a (plaintext) structure $DS$. The challenger executes $(K,EDS) \leftarrow \text{Setup}(1^k,DS)$ and outputs $EDS$ to $A$. Then adaptively chooses $m = \text{poly}(k)$ queries $Q_1, \ldots, Q_m$. For each query $Q_i$, the challenger executes $t_k \leftarrow \text{Token}(K,Q_i)$ and outputs token $t_k$ to $A$. Finally, $A$ returns a bit $b$ that is output by the experiment.

**Ideal$_{\Sigma,A,S}(k)$:** Given $z$, $A$ outputs a (plaintext) structure $DS$. The challenger outputs $z$ and the setup leakage $L_S(\Sigma,DS)$ to the simulator $S$. $S$ returns an encrypted data structure $EDS$ to $A$. Then adaptively chooses $m = \text{poly}(k)$ queries $Q_1, \ldots, Q_m$. For each query $Q_i$, the challenger gives $L_Q(\Sigma,Q_i)$ to $S$, and $S$ outputs a token $t_k$ to $A$. Finally, $A$ returns a bit $b$ that is output by the experiment.

We say that $\Sigma$ is adaptively $(L_S,L_Q)$-semantically secure if, for all PPT adversaries $A$, there exists a PPT simulator $S$ where

$$\Pr[Ideal_{\Sigma,A,S}(k) = 1] - \Pr[Real_{\Sigma,A}(k) = 1] \leq \text{negl}(k).$$

The definition of adaptive semantic security for interactive STE schemes is identical to Definition A.1 except that in the real experiment, for each query $Q_i$, the challenger $C$ executes the two-party protocol $\text{Query}_{C,A}((K,Q_i),EDS)$ with $A$, then outputs $\perp$ to $A$. Additionally, in the ideal experiment, $S$ may output a sequence of tokens to $A$ for each query $Q_i$.
B Formalization and Proof of Corollary 4.4

We first define a technical definition of equivalence between two plaintext aggregate range query schemes. Our equivalence definition captures when two plaintext aggregate range query schemes output exactly the same final aggregate result when given the same database and the same query.

**Definition B.1 (Equivalence).** Let \( \Pi_1 = (S_1, Q_1, R_1) \) and \( \Pi_2 = (S_2, Q_2, R_2) \) be two plaintext aggregate range query schemes. We say that \( \Pi_1 \) and \( \Pi_2 \) are equivalent plaintext aggregate range query schemes if, for all \( k \in \mathbb{N} \), for all \( \text{poly}(k) \)-size tables \( DB \), for all \( \text{poly}(k) \)-size sequences of queries \( Q_1, \ldots, Q_s \), for all queries \( Q \in Q_1, \ldots, Q_s \), given

\[
DS_i \leftarrow S_i(DB),
\]
\[
U_i \leftarrow Q_i(m, Q),
\]
\[
S_{i:0} \leftarrow \{DS_i[u] \mid u \in U_i\},
\]
\[
(st_{i:0}, R_{i:0}, U_{i:0}) \leftarrow R_i(\bot, m, Q, S_{i:0}).
\]

and, for all \( j > 0 \),

\[
(st_{i:j}, R_{i:j}, U_{i:j}) \leftarrow \begin{cases} R(st_{i:j-1}, m, Q, S_{i:j-1}) & \text{if } U_{i:j-1} \neq \bot \\ (\bot, R_{i:j-1}, \bot) & \text{if } U_{i:j-1} = \bot \end{cases}
\]

then there exists an integer \( k \geq 0 \) where \( R_{0:j} = R_{1:j} \) for \( j \geq k \).

We can then show that if a plaintext aggregate range query scheme is data independent, there exists an equivalent plaintext aggregate range query scheme that requires only one round of queries to the aggregate index structure.

**Corollary B.2.** Let \( \Pi = (S, Q, R) \) be a plaintext aggregate range query scheme. If \( \Pi \) is data independent, then there exists a scheme \( \Pi' = (S', Q', R') \) such that \( \Pi \) is equivalent to \( \Pi' \) and \( R' \) always outputs \( (st, R, U) \) where \( st = \bot \) and \( U = \bot \).

Due to space restrictions, we defer the full proof of Corollary B.2 to the full version.

C Query Type Transformations

In this section, we briefly describe how to transform certain aggregate range query schemes into another scheme that can answer a different type of aggregate query. Due to space restrictions, we omit the \( (S, Q, R) \) formalization and analysis of these transformations and defer those definitions to the full version.

**Transformations from range sum query.** Aggregate range query schemes for the encrypted range sum query problem may be used to answer *count*, *average*, and *variance* queries with a constant factor increase in storage, bandwidth, and time.

- **Count.** We add a “fake” attribute to each record with value 1, and apply the range sum query technique over this new attribute.
- **Average.** The client divides the result of a sum query over the desired range by the result of a count query over the same range.
- **Variance.** We add a new attribute to each record that holds the square of the desired query attribute, apply the range sum query technique over this new attribute, and then answer queries by taking the result of a sum query over the square attribute and subtracting the square of the result of an average query over the non-squared attribute.

**Transformations from range minimum query.** Aggregate range query schemes for the encrypted range minimum query problem may be used to answer *maximum*, *bottom-k*, and *top-k* queries.

- **Maximum.** We negate the value in the aggregate attribute and apply the range minimum query technique over the negated attribute. When receiving the result of a query, the client negates the returned value to return it to its original sign.
- **Bottom-k.** The technique we use is a generalization of the technique presented by Demertzis et al. [20]. Instead of creating one aggregate structure, we create \( k \) aggregate structures, where the \( i \)th structure stores the element of rank \( i \) (e.g., the first structure stores the true minimum for each preprocessed range, the second structure stores the value above the minimum for each preprocessed range, etc.). Additionally, each minimum is stored as a tuple, where the first element is the minimum value and the second element is an identifier that uniquely identifies the record that this minimum was associated with. During queries, the client generates \( O(k) \) search tokens for all of the \( k \)
structures, and $O(k)$ bandwidth is sent back to the client in response. The client then sorts the returned tokens, removes duplicate record IDs, and picks the lowest $k$ values.
- **Top-$k$.** Follows from a combination of the maximum and bottom-$k$ transformations.
- **Range.** We use a minimum and maximum structure, which gives us the difference between the maximum and minimum.

## D Extensions

### D.1 Higher Dimensions

The majority of the aggregate query schemes discussed in this paper easily generalize to $d$-dimensional databases of domain size $m_1 \times \cdots \times m_d$.

- **Sum:** For DPPDGP-SUM, a $d$-dimensional index can be created by using the $d$-dimensional prefix sums technique of [9], where an $d$-dimensional array of size $m_1 \times \cdots \times m_d$ is generated, and the index $(c_1, \ldots, c_d)$ stores the sum of all of the records in the $d$-dimensional hypercube defined by $(0, \ldots, 0)$ and $(c_1, \ldots, c_d)$. This requires the client to access $2^d$ entries in the structure.

- **Minimum and Mode:** For DPPDGP-Min1, DPPDGP-Min2, and LINEARMIN, we can construct $d$ indices, one for each dimension, and then constructing a new index where each entry stores the minimum of the “product” of the ranges represented by each entry of the $d$ dimension-specific indices. This requires the client to access $2^d$ entries in the final structure. (The same technique applies to the APPROXMODE schemes due to the similarities between the ST and AS structures.)

These generalizations do not work for the $\alpha$-APPROXMEDIAN and domain reduction schemes. The “bucketing” approach of both the median and the domain reduction schemes does not easily extend to higher dimensions since all such schemes operate by accessing a single entry in the encrypted structure. One may approximate these constructions using a single range cover-like approach used by Demertzis et al. [20] in their one-dimensional range search schemes; we leave further exploration of such extensions to future work.

### D.2 Record-Reporting

Applications that desire record-reporting for aggregate functions (specifically min/max and median) can instead (or additionally) encode the record identifier associated with the given plaintext value. For example, an encrypted search engine may be interested in identifying the top-$k$ documents with the highest word count that were generated within a particular date range. One can implement this via a combination of the query transformations detailed in Section C to reduce the top-$k$ problem to the minimum scheme; then encoding the record identifier of the document alongside each precomputed sub-aggregate in the structure. (To retrieve the actual record, a separate, $O(n)$-size index can be stored alongside the aggregate structure to map the record ID to the actual record.)

### D.3 Updates

We handle updates by combining a client-side update cache (e.g., [64]) with periodic intermediate Setup and “rebuild” operations. At a high-level, we initialize the cache to have a size of $\delta_1$ (a tunable parameter). Then, when the client wants to add or change a record, they add the change to their client-side cache without propagating it to the server immediately. On subsequent range queries, the client is responsible for performing a linear scan of the cache to detect if any of the updates fall within the queried range and adjusting the computed aggregate accordingly. Once the cache size reaches $\delta_1$, the client triggers a Setup operation where they generate a new encrypted structure over only the records in the cache and then send the new structure to the server, which accumulates multiple such update structures over time. The client stores the keys for the new structure alongside the previously stored keys and empties the cache. On subsequent queries, the client generates multiple search tokens for both structures. To avoid a continual increase in the number of stored structures and search tokens, the client periodically rebuilds the server-side structure when the number of update structures reaches $\delta_2$ by constructing a new, single index based off of queries to the existing structures on the server. The client then sends the new structure to the server, which then deletes the previous structures and replaces it with the new index.