
Alexandra Henzinger
MIT
Matthew M. Hong
MIT
Henry Corrigan-Gibbs
MIT
Sarah Meiklejohn
Google
Vinod Vaikuntanathan
MIT

Abstract. We present SimplePIR, the fastest single-server private information retrieval scheme known to date. SimplePIR’s security holds under the learning-with-errors assumption. To answer a client’s query, the SimplePIR server performs fewer than one 32-bit multiplication and one 32-bit addition per database byte. SimplePIR achieves 10 GB/s/core server throughput, which approaches the memory bandwidth of the machine and the performance of the fastest two-server private-information-retrieval schemes (which require non-colluding servers). SimplePIR has relatively large communication costs: to make queries to a 1 GB database, the client must download a 121 MB “hint” about the database contents; thereafter, the client may make an unbounded number of queries, each requiring 242 KB of communication. We present a second single-server scheme, DoublePIR, that shrinks the hint to 16 MB at the cost of slightly higher per-query communication (345 KB) and slightly lower throughput (7.4 GB/s/core). Finally, we apply our new private-information-retrieval schemes, together with a novel data structure for approximate set membership, to the task of private auditing in Certificate Transparency. We achieve a strictly stronger notion of privacy than Google Chrome’s current approach with modest communication overheads: 16 MB of download per month, along with 150 bytes per TLS connection.

1 Introduction

In a private information retrieval (PIR) protocol [27,62], a database server holds an array of $N$ records. A client wants to fetch record $i \in \{1, \ldots, N\}$ from the server, without revealing the index $i$ that it desires to the server. PIR has applications to systems for private database search [85,93], metadata-hiding messaging [9,10], private media consumption [55], credential breach reporting [66,82,91,94], private contact discovery [60], privacy-friendly advertising [11,54,58,87], and private blocklist lookups [61], among others.

Modern PIR schemes require surprisingly little communication: with a single database server and under modest cryptographic assumptions [21,49,80], the total communication required to fetch a database record grows only polylogarithmically with the number of records, $N$. Unfortunately, PIR schemes are computationally expensive: the server must touch every bit of the database to answer even a single client query [13], since otherwise the PIR scheme leaks information about which database records the client is not interested in. (A number of recent PIR schemes preprocess the database such that the server can answer a query in time sublinear in $N$, but all known approaches require either client-specific preprocessing [30,31,61,88,97] or impractically large server storage [13,17,22].) Thus, a hard limit on the throughput of PIR schemes—that is, the ratio between the database size and the server time to answer a query—is the speed with which the PIR server can read the database from memory: roughly 12.4 GB/s/core on our machine [92].

In the standard setting, in which the client interacts with a single database server, the performance of existing PIR protocols is far from this theoretical limit: we measure that the fastest prior single-server PIR schemes [76] achieve a throughput of 259 MB/s/core, or 2% of our machine’s memory bandwidth, on a database of hundred-byte records. It is possible to push the performance up to 1.3 GB/s/core when the database records are hundreds of kilobytes long, though that parameter setting is not relevant for many PIR applications, including our application to Certificate Transparency.

When the client can communicate with multiple non-colluding database servers [27], there exist PIR schemes with server-side throughput of up to 11.5 GB/s/core, or 93% of the memory bandwidth (described in Table 1). However, these multi-server PIR schemes are cumbersome to deploy, since they rely on multiple coordinating yet independent infrastructure providers. In addition, their security is brittle, as it stems from a non-collusion assumption rather than from cryptographic hardness. Thus, existing PIR schemes suffer from either poor performance—in the single-server setting—or undesirable trust assumptions—in the multi-server case.

In this paper, we present two new single-server PIR schemes that exceed the throughput of all existing single-server PIR protocols and approach the throughput of multi-server ones. In addition, our schemes are relatively simple to explain and easy to implement: our complete implementation of both schemes, available at github.com/ahenzinger/simplepir, requires roughly 1,400 lines of Go code, plus 200 lines of C, and uses no external libraries.

More specifically, our first scheme, SimplePIR, achieves a server throughput of 10 GB/s/core, or 81% of the memory...
bandwidth, though it requires the client to download a relatively large “hint” about the database contents before making its queries. On a database of $N$ bytes, the hint has size roughly $4\sqrt{N}$ KB. The hint is not client-specific, and a client can reuse the hint over many queries, so the amortized communication cost per query can be small. Our second scheme, DoublePIR, achieves slightly lower server throughput of 7.4 GB/s/core, but shrinks the hint to roughly 16 MB for a database of one-byte records—indeed, independent of the number of records in the database.

Our techniques. We now summarize the technical ideas behind our results.

Recap: Single-server PIR. Our starting point is the single-server PIR construction of Kushilevitz and Ostrovsky [62]. In their scheme, the PIR server represents an $N$-record database as a matrix $D$ of dimension $\sqrt{N}$ by $\sqrt{N}$. To fetch the database record in row $i$ and column $j$, the client sends the server the encryption $E(q)$ of a dimension-$\sqrt{N}$ vector that is zero everywhere except that it has a “1” in index $j$. If the encryption scheme is linearly homomorphic, the server can compute the matrix-vector product $D \cdot E(q) = E(D \cdot q)$ under encryption and return the result to the client. The client decrypts to recover $D \cdot q$ which, by construction, is the $j$-th column of the database, as desired. The total communication grows as $\sqrt{N}$.

SimplePIR from linearly homomorphic encryption with preprocessing. The PIR server’s throughput here is limited by the speed with which it can compute the product of the plaintext matrix $D$ with the encrypted vector $E(q)$. Our observation in SimplePIR (Section 4) is that, using Regev’s learning-with-errors-based encryption scheme [86], the server can perform the vast majority of the work of computing the matrix-vector product $D \cdot E(q)$ \textit{in advance}—before the client even makes its query. The server’s preprocessing depends only on the database $D$ and the public parameters of the Regev encryption scheme, so the server can reuse this preprocessing work across many queries from many independent clients. After this preprocessing step, to answer a client’s query, the server needs to compute only roughly $N$ 32-bit integer multiplications and additions on a database of $N$ bytes. The catch is that the client must download a “hint” about the database contents after this preprocessing step—the hint accounts for the bulk of the communication cost in SimplePIR.

DoublePIR from one recursive step. The idea behind DoublePIR (Section 5) comes from the original Kushilevitz and Ostrovsky paper [62]: in SimplePIR, the client downloads the hint from the server, along with a dimension-$\sqrt{N}$ encrypted vector. However, to recover its record of interest, the client only needs one small part of the hint and one component of this vector. We show how the client can use SimplePIR recursively on the hint and this vector to fetch its desired database record at a reduced communication cost. To minimize the concrete costs, we make non-black-box use of SimplePIR in this recursive construction, which saves a factor of the lattice dimension, which is 1024 for our parameters, over a naïve design.

Application to Certificate Transparency. Finally, we evaluate our PIR schemes in the context of the application of signed certificate timestamp (SCT) auditing in Certificate Transparency. In this auditing application, a server holds a set $S$ of strings and a client (web browser) wants to test whether a particular string $\sigma$, representing an SCT, appears in the set $S$, while hiding $\sigma$ from the server. (The string $\sigma$ reveals information about which websites a client has visited.) Google Chrome currently implements this auditing step using a solution that provides $k$-anonymity for $k = 1000$ [35].

Along the way, we construct a new data structure (Section 6) for more efficiently solving this type of private set-membership problem using PIR, when a constant rate of false positives is acceptable (as in our application). In this setting, standard Bloom filters [15] and approaches based on PIR by keywords [26] require the client to perform PIR over a database of $\lambda N$ bits (if the set $S$ has size $N$ and $\lambda \approx 128$ is a security parameter). In contrast, our data structure requires performing PIR over only $8N$ bits—giving a roughly 16x speedup in our application.

Google’s current solution to SCT auditing, which provides $k$-anonymity rather than full cryptographic privacy, requires the client to communicate 24 B on average per TLS connection. Our solution, which provides cryptographic privacy, requires 150 B and 0.0003 core-seconds of server compute on average per TLS connection, along with 16 MB of client download and 150 KB of client storage every month to maintain the hint.

Limitations. Our new PIR schemes come with two main downsides. First, our client must download a “hint”: on databases gigabytes in size, the hint is tens of megabytes. If a client makes only one query, this hint download dominates the overall communication. Second, our schemes’ online communication is on the order of hundreds of kilobytes, which is 10x larger than in some prior work. Nevertheless, we believe that SimplePIR and DoublePIR represent an exciting new point in the PIR design space: large computation savings, along with a conceptually simple design and small, stand-alone codebase, at the cost of modest communication and storage overheads.

Our contributions. In summary, our contributions are:

• two new high-throughput single-server private information retrieval protocols (Sections 4 and 5),
• a new data structure for private set membership using PIR (Section 6) and its application to private auditing in Certificate Transparency (Section 7), and
• the evaluation of these schemes, using a new open-source implementation (Section 8).

2 Related work and comparison

Chor, Goldreich, Kushilevitz and Sudan [27] introduced PIR in the multi-server setting and Kushilevitz and Ostrovsky [62] gave the first construction of single-server PIR. Their scheme uses a linearly homomorphic encryption scheme that expands
Lattice-based PIR. To drive down this computational cost, recent PIR schemes instantiate the Kushilevitz-Ostrovsky construction using encryption schemes based on the ring learning-with-errors problem ("Ring LWE") [72]. In these schemes, for each bit of the database, the server performs work polylogarithmic in the security parameter—rather than polynomial.

However, these savings in computation come at the cost of a larger expansion factor \( F \approx 10 \), which increases the communication as the dimension parameter \( d \) cannot be too large. For example, XPIR [5] takes \( d = 2 \). In addition, the client in the Kushilevitz-Ostrovsky scheme must upload \( N^{1/d} \) ciphertexts, and each ring-LWE ciphertext is at least thousands of kilobytes in size. This imposes large absolute communication costs (e.g., tens of MB per query, on a database of hundreds of MB).

SealPIR [9] shows that the client can compress the ciphertexts in an XPIR-style scheme before uploading them. The server can then expand these ciphertexts using homomorphic operations. (FastPIR [6] uses a similar idea to compress responses.) This optimization reduces the communication costs by orders of magnitude, though it requires the server to store some per-client information ("key-switching hints")—essentially, encryptions of the client’s secret decryption key—that is megabytes in size and that the client must upload to the server before it makes any queries.

MulPIR [8], OnionPIR [77], and Spiral [76] additionally use fully homomorphic encryption [47] to reduce the communication cost. In Spiral [76], for example, the cost grows roughly as \( N^{1/d} F \), where the exponent on the \( F \) term is now 1 instead of \( d - 1 \). Building on ideas of Gentry and Halevi [48], Spiral shows how to decrease the communication cost while keeping the throughput high: up to 259 MB/s on a database of short records. (With long database records, Spiral does not use the SealPIR query compression technique and gets throughput as large as 1,314 MB/s, at the cost of increased communication.)

Plain learning with errors. We base our PIR schemes on the standard learning-with-errors (LWE) problem—not the ring variant. The expansion factor of the standard LWE-based encryption scheme, Regev encryption [86], is roughly \( F = n \approx 1024 \), where \( n \) is the lattice security parameter. This large expansion factor means that a direct application of Regev encryption to the Kushilevitz-Ostrovsky PIR scheme would be disastrous in terms of communication and computation. Our innovation is to show that the server can do the bulk of its work in advance, and reuse it over multiple clients.

Aside from the fact that our scheme is based on a weaker cryptographic assumption, namely plain LWE as opposed to ring LWE, this strategy yields multiple benefits:

1. Our LWE-based schemes are simple to implement: they require no polynomial arithmetic or fast Fourier transforms.
2. Our schemes do not require the server to store any extra per-client state. In contrast, many schemes based on Ring LWE [8, 9, 76, 77] rely on optimizations that require the server to store one “key-switching hint” for each client.
3. Our schemes are faster. We avoid the costs associated with ciphertext compression and expansion. In addition, since we only need our encryption scheme to be linearly (not fully) homomorphic, we can use smaller and more efficient lattice parameters.

The drawback of our schemes is that they have larger com-
munition cost, especially when the client makes only a single query (so the client cannot amortize the offline download cost over multiple queries) or when the database records are long.

**Concurrent work: FrodoPIR.** FrodoPIR [34] is independent concurrent work that constructs a PIR scheme that is essentially identical to SimplePIR. The default configuration of FrodoPIR has communication cost $O(N)$, on database size $N$, though rebalancing the scheme gives a $O(n\sqrt{N})$-cost, on lattice dimension $n$, as in SimplePIR. The additional contributions of our work are: the more communication-efficient DoublePIR scheme, our new data structure for private set-membership queries (Section 6), the application to certificate transparency (Section 7), and an optimized implementation of our schemes.

**Preprocessing and PIR.** The server in our PIR schemes performs some client-independent preprocessing. Prior work uses server-side preprocessing—either one-time [13, 17, 22] or per-client [30, 31, 61, 88, 97]—to build PIR where the server online work is sublinear in the database size. Prior work also proves strong lower bounds on the performance of any such PIR with preprocessing schemes [13, 30, 31, 84]. In contrast, in this work, we use preprocessing to build PIR where the amortized per-query server work is still linear, but it is concretely efficient.

**Multi-server PIR.** In our PIR schemes, the client communicates with a single database server. In multi-server PIR schemes [27], the client communicates with multiple database servers and client privacy holds only as long an attacker cannot compromise some number of them. In Table 1, we give the throughput of an optimized implementation [59] of a two-server PIR scheme based on distributed point functions (“DPF PIR”) [16, 50]. We also report the throughput of a $\sqrt{N}$-communication two-server PIR scheme (“XOR PIR”) [27]. It is possible to speed these schemes up by roughly 2x if the server’s running time can depend on the Hamming weight of the client’s query vector (“XOR PIR fast”). The downside of this optimization is that it could potentially leak information about one server’s secret query vector to another server via timing information, thereby breaking client privacy. Whether such a performance-leakage trade-off is acceptable in practice likely depends on the application scenario.

**Hardware acceleration for PIR.** Recent work improves the throughput of both single-server [67] and multi-server [56] PIR using hardware acceleration. This approach is complementary to ours, as it may further speed up our new PIR protocols.

**Privacy and certificate transparency.** Lueks and Goldberg [71] and Kales, Omolola, and Ramacher [59] propose using multi-server PIR for auditing in certificate transparency. We work in the single-server setting, where the client communicates with a separate audit server (e.g., Google, in the application to Chrome). Further, we introduce a new set-membership data structure to reduce the cost of auditing (Section 6). We discuss existing approaches to auditing in Section 7.

## 3 Background and definitions

**Notation.** For a probability distribution $\chi$, we use $x \leftarrow \chi$ to indicate that $x$ is a random sample from $\chi$. For a finite set $S$, we use $x \leftarrow S$ to denote sampling $x$ uniformly at random from $S$. We use $\mathbb{N}$ to represent the natural numbers and $\mathbb{Z}_p$ to represent integers modulo $p$. All logarithms are to the base two. For $x \in \mathbb{N}$, we let $\lfloor x \rfloor$ denote the set $\{1, \ldots, x\}$. Throughout, we assume that values like $\sqrt{N}$ are integral, wherever doing so is essentially without loss of generality. Algorithms are modeled as RAM programs and their runtime is measured in terms of the number of RAM instructions executed. We use the symbols MB and GB to denote $2^{20}$ and $2^{30}$ bytes, respectively.

### 3.1 Learning with errors (LWE)

The security of our PIR schemes relies on the decision version of the learning-with-errors assumption [86]. The assumption is parameterized by the dimension of the LWE secret $n \in \mathbb{N}$, the number of samples $m \in \mathbb{N}$, the integer modulus $q \geq 2$, and an error distribution $\chi$ over $\mathbb{Z}$. The LWE assumption then asserts that for a matrix $A \leftarrow \mathbb{Z}_q^m$, a secret $s \leftarrow \mathbb{Z}_q^n$, an error vector $e \leftarrow \mathbb{Z}_q^m$, and a random vector $r \leftarrow \mathbb{Z}_q^m$, the following distributions are computationally indistinguishable:

$$
\{(A, As + e)\} \approx \{(A, r)\}.
$$

More specifically, the $(n, q, \chi)$-LWE problem with $m$ samples is $(T, e)$-hard if all adversaries running in time $T$ have advantage at most $e$ in distinguishing the two distributions. In Section 4.2, we give concrete values for the LWE parameters.

**Secret-key Regev encryption.** Regev [86] gives a secret-key encryption scheme that is secure under the LWE assumption. With LWE parameters $(n, q, \chi)$ and a plaintext modulus $p$, the Regev secret key is a vector $s \leftarrow \mathbb{Z}_q^n$. The Regev encryption of a message $\mu \in \mathbb{Z}_p$ is

$$
(a, c) = (a, as + e + \lfloor q/p \rfloor \cdot \mu) \in \mathbb{Z}_q^n \times \mathbb{Z}_q,
$$

for $e \leftarrow \chi$. To decrypt the ciphertext, anyone who knows the secret $s$ can compute $c - as \mod q$ and round the result to the nearest multiple of $\lfloor q/p \rfloor$. Decryption succeeds as long as the absolute value of the error sampled from the error distribution $\chi$ is smaller than $\frac{1}{2} \cdot \lfloor q/p \rfloor$. We say that a setting of the Regev parameters supports correctness error $\delta$ if the probability of a decryption error is at most $\delta$ (over the encryption algorithm’s randomness). Regev encryption is additively homomorphic, since given two ciphertexts $(a_1, c_1)$ and $(a_2, c_2)$, their sum $(a_1 + a_2, c_1 + c_2)$ decrypts to the sum of the plaintexts, provided again that the error remains sufficiently small.

### 3.2 Private information retrieval with hints

We now give the syntax and security definitions for the type of PIR schemes we construct. Our form of PIR is very similar to the standard single-server PIR schemes [27, 62]. The primary
distinction is that we allow the PIR server to preprocess the database ahead of time and to output two ‘hints’: one that the server stores locally, and another that the server sends to each client. This preprocessing allows the PIR server to push much of its computational work into an offline phase that takes place before the client makes its query. In our constructions, both hints are small—they have size sublinear in the database size. In addition, all clients use the same hint and a client can reuse the same hint for all of its PIR queries.

Remark 3.1 (Handling database updates). As PIR schemes with preprocessing perform some precomputation over the database, the server inherently needs to repeat some of this work if the database contents change. Related work investigates how to minimize the amount of computation and communication that such database updates incur, in both a black-box [61] and a protocol-specific [73] manner. We address how to handle updates in our schemes in Appendices C.3 and E.3.

A PIR-with-preprocessing scheme [13], over plaintext space $\mathcal{D}$ and database size $N \in \mathbb{N}$, consists of four routines, which all take the security parameter as an implicit input:

$\text{Setup}(\text{db}) \rightarrow (\text{hint}_s, \text{hint}_c)$. Given a database $\text{db} \in \mathcal{D}^N$, output preprocessed hints for the server and the client.

$\text{Query}(i) \rightarrow (\text{st}, \text{qu})$. Given an index $i \in [N]$, output a secret client state $\text{st}$ and a database query $\text{qu}$.

$\text{Answer}(\text{db}, \text{hint}_s, \text{qu}) \rightarrow \text{ans}$. Given the database $\text{db}$, a server hint $\text{hint}_s$, and a client query $\text{qu}$, output an answer $\text{ans}$.

$\text{Recover}(\text{st}, \text{hint}_c, \text{ans}) \rightarrow d$. Given a secret client state $\text{st}$, a client hint $\text{hint}_c$, and an answer $\text{ans}$, output a record $d \in \mathcal{D}$.

Correctness. When the client and the server execute the PIR protocol faithfully, the client should recover its desired database record with all but negligible probability in the implicit correctness parameter. Formally, we say that a PIR scheme has correctness error $\delta$ if, on database size $N \in \mathbb{N}$, for all databases $\text{db} = (d_1, \ldots, d_N) \in \mathcal{D}^N$ and for all indices $i \in [N]$, the following probability is at least $1-\delta$:

$$\Pr \left[ \begin{array}{l}
\text{Pr}\left[d_i = \hat{d}_i: \begin{array}{l}
(\text{hint}_s, \text{hint}_c) \leftarrow \text{Setup}(\text{db}) \\
(\text{st}, \text{qu}) \leftarrow \text{Query}(i) \\
\text{ans} \leftarrow \text{Answer}(\text{db}, \text{hint}_s, \text{qu}) \\
\hat{d}_i \leftarrow \text{Recover}(\text{st}, \text{hint}_c, \text{ans})
\end{array} \right] \rightarrow 1\right] \leq \epsilon.
\right]$$

For the PIR scheme to be non-trivial, the total client-to-server communication should be smaller than the bitlength of the database. That is, it must hold that $|\text{hint}_c| + |\text{qu}| + |\text{ans}| \ll |\text{db}|$.

Security. The client’s query should reveal no information about its desired database record. That is, we say that a PIR scheme is $(T, \epsilon)$-secure if, for all adversaries $\mathcal{A}$ running in time at most $T$, on database size $N \in \mathbb{N}$, and for all $i, j \in [N]$,

$$\Pr[\mathcal{A}(1^N, \text{qu}) = 1: (\text{st}, \text{qu}) \leftarrow \text{Query}(i)] - \Pr[\mathcal{A}(1^N, \text{qu}) = 1: (\text{st}, \text{qu}) \leftarrow \text{Query}(j)] \leq \epsilon.$$
vector to the server. The server computes the matrix-vector product between the database and the query vector and returns it to the client. Finally, the client decrypts element $i_{\text{row}}$ of the server’s answer vector—which corresponds exactly to the inner product of database row $i_{\text{row}}$ and encrypted unit vector $u_{i_{\text{col}}}$, or, equivalently, the encrypted database entry at $(i_{\text{row}}, i_{\text{col}})$. In this scheme, the server and the client exchange $2\sqrt{N}$ ciphertext elements, while the server performs $N$ ciphertext multiplications and additions to answer each PIR query.

Our starting point is to instantiate this “square-root” approach with the secret-key version of Regev’s LWE-based encryption scheme [86]. Let $(n, q, \chi)$ be LWE parameters. Then, the Regev encryption of a vector $\mathbf{v} \in \mathbb{Z}_q^n$ consists of a pair of a matrix and a vector:

$$\text{Enc}(\mathbf{v}) = (A, \mathbf{c}) = (A, A \mathbf{s} + e + [q/p] \cdot \mathbf{v}),$$

for some LWE matrix $A \in \mathbb{Z}_{q}^{m \times n}$, secret $s \in \mathbb{Z}_{q}^n$, and error vector $e \in \mathbb{Z}_q^m$.

We make three crucial observations about Regev encryption:

1. First, a large part of the ciphertext—namely, the matrix

$$A = (A_{11}, A_{12}, \ldots, A_{m1}, A_{m2}, \ldots, A_{mn}),$$

is independent of the encrypted message. It is thus possible to generate the matrix $A$ ahead of time.

2. Second, Regev encryption remains secure even when the same matrix $A$ is used to encrypt polynomially many messages (cf. Corollary C.3), provided that each ciphertext uses an independent secret vector $s$ and error vector $e$ [83].

3. Finally, we can take $A$ to be pseudorandom (rather than random) at a negligible loss in security, allowing us to succinctly represent $A$ by a short random seed.

In SimplePIR, we leverage these three observations as follows. Consider a client who wishes to retrieve the database entry at $(i_{\text{row}}, i_{\text{col}})$. At a conceptual level, the client’s query to the server consists of $\mathbf{Enc}(u_{i_{\text{col}}}) = (A, \mathbf{c})$—the Regev encryption of the vector $u_{i_{\text{col}}}$, which is zero everywhere but with a “1” at index $i_{\text{col}}$. The server then represents the database as a matrix $D \in \mathbb{Z}_q^{N \times n}$ and computes and returns the matrix-vector product of the database with the client’s encrypted query, i.e., $(D \cdot A, D \cdot \mathbf{c})$. From the server’s reply, the client can use standard Regev decryption to recover $D \cdot u_{i_{\text{col}}} \in \mathbb{Z}_q^n$, which is exactly the $i_{\text{col}}$-th column of the database, as desired.

Now, we make the following modifications:

1. We have the server compute the value $D \cdot A$ ahead of time in a preprocessing phase. This preprocessing step requires $2nN$ operations in $\mathbb{Z}_q$, on lattice dimension $n \approx 2^{10}$ and database size $N$. Then, to answer the client’s query, the server needs to compute the value $D \cdot \mathbf{c}$, which requires only $2N$ operations in $\mathbb{Z}_q$. So, an $n/(n+1)$ fraction (i.e., 99.9%) of the server’s work can happen ahead of time—before the client even decides which database record it wants to fetch.

2. We have all clients use the same matrix $A$ to build each of their queries. Then, the server only precomputes $D \cdot A$ once. The server sends this one-time “hint” to all clients. Thus, the server amortizes the cost of computing and communicating $D \cdot A$ over many clients and over many queries.

3. As an optimization, we compress $A$ using pseudorandomness. Specifically, the server and the clients can derive $A$ as the output of a public hash function, modelled as a random oracle, applied to a fixed string in counter mode. This saves on bandwidth and storage, as the server and the clients...
We discuss parameter selection further in Appendix C.1.

4.2 Parameter selection

Picking the LWE parameters \((n, q, \chi)\) and the plaintext modulus \(p\) requires a standard (though tedious) analysis. We choose our parameters to have 128-bit security, according to modern lattice-attack-cost estimates [7]. In particular, we set the secret dimension \(n = 2^{10}\), use modulus \(q = 2^{32}\) (as modern hardware natively supports operations with this modulus), set the error distribution \(\chi\) to be the discrete Gaussian distribution with standard deviation \(\sigma = 6.4\), and allow correctness error \(\delta = 2^{-40}\). We obtain the following trade-off between database size \(N\) and plaintext modulus \(p\):

<table>
<thead>
<tr>
<th>Database size (N)</th>
<th>2^26</th>
<th>2^28</th>
<th>2^30</th>
<th>2^34</th>
<th>2^38</th>
<th>2^42</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext modulus (p)</td>
<td>991</td>
<td>833</td>
<td>701</td>
<td>495</td>
<td>350</td>
<td>247</td>
</tr>
</tbody>
</table>

We discuss parameter selection further in Appendix C.1.

4.3 Extensions

Finally, we extend our SimplePIR construction to meet the requirements of realistic deployment scenarios:

Supporting databases with larger record sizes. The basic SimplePIR scheme (Figure 2) supports a database in which each record is a single \(\mathbb{Z}_p\) element—or, roughly 8-10 bits with our parameter settings. Our main application (Section 7) uses a database with one-bit records, though other applications of PIR [6, 9, 10, 55, 76] use much longer records.

To handle large records, we observe that the client in SimplePIR can retrieve an entire column of the database at once. Concretely, after executing a single online phase with the server to query for database element \((i_{row}, i_{col})\), the client can run the Recover procedure \(\sqrt{N}\) times—one for every row in \([\sqrt{N}]\)—to reconstruct the entire column \(i_{col}\) of the database matrix. So, to support large records, we encode each record as multiple elements in the plaintext space, \(\mathbb{Z}_p\), and store these elements stacked vertically in the same column. By making a single online query and reconstructing the corresponding column of elements, the client then recovers any record of its choosing.

On a database of \(N\) records, each in \(\mathbb{Z}_p^d\) (where \(d \leq N\)), with LWE secret dimension \(n\) and modulus \(q\), SimplePIR has:

- one-time (hint) download \(n \cdot \sqrt{dN}\) elements in \(\mathbb{Z}_q\),
- per-query upload and download \(\sqrt{dN}\) elements in \(\mathbb{Z}_q\), and
- per-query server computation \(2dN\) operations in \(\mathbb{Z}_q\).

Fetched many database records at once (“Batch PIR”).

In many applications [9, 10], a client wants to fetch \(k\) records from the PIR server at once. If the client runs our PIR protocol \(k\) times on a database of \(N\) records, the total server time would be roughly \(kN\). We can apply the “batch PIR” techniques of Ishai et al. [57] to allow a client to fetch \(k\) records at server-side cost \(\ll kN\), without increasing the hint size.

The idea is to randomly partition the database of \(N\) records into \(k\) chunks, each represented as a matrix of dimension \((\sqrt{N}/k)\)-by-\(\sqrt{N}\). If the \(k\) records that the client wants to fetch fall into distinct chunks, the client can recover these records by running SimplePIR once on each database chunk. In this case, the hint size remains \(n\sqrt{N}\)—as in one-query SimplePIR. The communication cost for the client is \(k\sqrt{N}\) times larger than in one-query SimplePIR (and identical to the communication if the client fetched all \(k\) records sequentially). The server performs \(N\) operations in \(\mathbb{Z}_q\)—as in one-query SimplePIR.

However, more than one of the client’s desired records may fall into the same chunk. There are two ways to handle this:

- If the client must recover all \(k\) records with overwhelming probability, the client can make \(\lambda\) PIR queries to each of the \(k\) chunks to achieve failure probability \(2^{-\Omega(1)}\) [9, 57]. This optimization saves on server work as long as \(\lambda < k\).
- If the client only needs to recover a constant fraction of the \(k\) database records, then the client and the server can run this batch-PIR protocol only once. The server-side computation cost is as in one-query SimplePIR.

Additional improvements. We discuss how to further improve the asymptotic efficiency of SimplePIR in Appendix C.3.

4.4 Fast linearly homomorphic encryption

In Appendix D, we introduce the notion of linearly homomorphic encryption with preprocessing. This new primitive abstracts out the key properties of Regev encryption that we use in SimplePIR. We expect this new form of linearly homomorphic encryption to have further practical applications.

5 DoublePIR

While SimplePIR has high server-side throughput, it requires the client to download and store a relatively large preprocessed hint, of size roughly \(n\sqrt{N}\) on lattice dimension \(n \approx 2^{10}\) and database size \(N\). In this section, we present DoublePIR, a new PIR scheme that recursively applies SimplePIR to reduce the hint size to roughly \(n^2\) on lattice dimension \(n\)—independent of the database size—while maintaining a server-side throughput upwards of 7.4 GB/s. (In practice, this hint size is 16 MB for one-byte records.) For databases of very many records \((N \gg n^2 \approx 2^{20})\), DoublePIR has a much smaller hint size than SimplePIR. As in SimplePIR, the per-query communication cost for DoublePIR is \(O(\sqrt{N})\) on database size \(N\).

5.1 Construction

We present a formal description of DoublePIR in Figure 14 of Appendix E, along with a full correctness and security analysis.
In this section, we describe the key design ideas.

We first give the concrete costs of DoublePIR on database size $N$, lattice dimension $n$, LWE modulus $q$, plaintext modulus $p$, and $\kappa = \lfloor \log(q)/\log(p) \rfloor \approx 4$ (chosen as in Appendix E.1).

In a one-time public preprocessing phase, DoublePIR requires

1. the server to perform $2nN + 2n^2\sqrt{N}$ operations in $\mathbb{Z}_q$, and
2. the client to download $kn^2$ elements in $\mathbb{Z}_q$.

On each query, DoublePIR requires

1. the client to upload $2\sqrt{N}$ elements in $\mathbb{Z}_q$,
2. the server to do $2N + 2(2n + 1) \cdot \sqrt{N} \cdot \kappa$ $\mathbb{Z}_q$ operations, and
3. the client to download $(2n + 1) \cdot \kappa$ elements in $\mathbb{Z}_q$.

At a high level, DoublePIR first executes exactly as SimplePIR: from the database, the server computes a hint matrix and, in response to each client’s query, produces an answer vector. At this point, we observe that a client querying for element $(i_{row}, i_{col})$ in SimplePIR needs two pieces of information to recover its desired database element:

- row $i_{row}$ of the hint matrix $D \cdot A \in \mathbb{Z}_q^{N \times n}$, and
- element $i_{col}$ of the answer vector $a \in \mathbb{Z}_q^N$.

Thus, in DoublePIR, we have the client execute a second level of SimplePIR over the hint matrix and the answer vector to retrieve these $(n + 1)$ values. As such, the client in DoublePIR recovers the database entry at $(i_{row}, i_{col})$ without downloading the large first-level hint.

Kushilevitz and Ostrovsky [62] first proposed using recursion to reduce communication costs in PIR in this way. However, applied naively, this strategy requires $(n + 1) \approx 2^{10}$ instances of PIR to recover the $(n + 1)$ desired values. We avoid this bottleneck with the insight that SimplePIR sets the client retrieve a column of the database at a time (as discussed in Section 4.3). Therefore, in DoublePIR, we run the second level of PIR over the database corresponding to the transpose of the hint matrix concatenated with the answer vector (i.e., $[D \cdot A \parallel a]^T$). Using a single invocation of SimplePIR, the client in DoublePIR can retrieve column $i_{row}$ of this database—which holds exactly row $i_{row}$ of the hint matrix and element $i_{col}$ of the answer vector—and finally recover the database entry at $(i_{row}, i_{col})$. As SimplePIR executes over a database of elements in $\mathbb{Z}_p$, while the hint matrix and the answer vector consist of elements in $\mathbb{Z}_q$, the server in DoublePIR computes the base-$p$ decomposition of the entries in the hint matrix and the answer vector before performing the second level of PIR.

Since this second level of PIR operates on a much smaller database, its cost is dwarfed by that of the first level of PIR: in DoublePIR, both the online communication and the server throughput remain roughly the same as in SimplePIR. Moreover, as the client in DoublePIR forgoes downloading the large first-level hint, it now only downloads a much smaller hint, whose size is independent of the database length, produced by the second level of PIR. Concretely, our PIR client downloads a 16 MB hint in the offline phase.

Remark 5.1 (Why not recurse more?). DoublePIR performs two levels of PIR to reduce the total communication. A natural question is whether additional levels of recursion can help, as in standard single-server PIR schemes [62]. After $r$ levels of recursion, the cost of the recursive PIR scheme, on lattice dimension $n$ and database size $N$, would be (hiding constants):

- one-time download $n^r$ in the preprocessing step, as well as
- per-query upload $r \cdot N^{1/r}$ and download $n^{r-1}$.

For $r > 2$, the communication is likely too large for databases of interest. An intriguing open question is to construct recursive LWE-based PIR schemes with total communication $n \cdot N^{1/r}$.

5.2 Extensions

We extend DoublePIR to handle diverse deployment scenarios.

Handling large database records. To handle databases with large records, we represent each record as a series of elements in $\mathbb{Z}_{p'}$, where $p$ is the plaintext modulus, using base-$p$ decomposition. Let $d$ denote the number of $\mathbb{Z}_{p'}$ elements that each record maps to. Then, on each execution of DoublePIR, we run the PIR scheme $d$ times in parallel, over $d$ databases, where the $i$-th database holds the $i$-th $\mathbb{Z}_{p'}$ element of each record. With this approach, DoublePIR’s throughput is identical on databases with long records and with short records. On a database of $N$ records, each in $\mathbb{Z}_{p'}^d$, with lattice dimension $n$, LWE modulus $q$, and $\kappa = \lfloor \log(q)/\log(p) \rfloor$, DoublePIR has:

- hint size $dkn^2$ elements in $\mathbb{Z}_q$,
- online upload $2\sqrt{N}$ elements in $\mathbb{Z}_q$,
- online server work $2d \left( N + \kappa(2n + 1) \sqrt{N} \right)$ ops. in $\mathbb{Z}_q$, and
- online download $dk \cdot (2n + 1)$ elements in $\mathbb{Z}_q$.

Batching client queries. To implement query batching in DoublePIR, we batch queries exactly as in SimplePIR when performing the first level of PIR. As DoublePIR makes non-black-box use of SimplePIR in performing the second level of PIR, we are not able to derive any computation savings from batching in this second, recursive step. (In particular, in the second level of PIR, the client must read an entire column consisting of $(n+1)$ elements at once for each query; this breaks SimplePIR’s batching trick.) However, as the first level of PIR dominates the computation in DoublePIR, batching many queries nevertheless greatly improves DoublePIR’s throughput.

Concretely, to fetch a constant fraction among a set of $k$ records from a database of $N$ values in $\mathbb{Z}_{p'}$, on lattice dimension $n$, LWE modulus $q$, and $\kappa = \lfloor \log(q)/\log(p) \rfloor$, DoublePIR has:

- hint size $kn^2$ elements in $\mathbb{Z}_q$,
- online upload $\sqrt{N}(k + \sqrt{k})$ elements in $\mathbb{Z}_q$,
- online server work $2N + 2k(2n + 1)\sqrt{N}$ ops. in $\mathbb{Z}_q$, and
- online download $k(2n + 1)$ elements in $\mathbb{Z}_q$. 

8
6 Data structure for private approximate set membership

In this section, we introduce a new data structure for the private approximate set membership problem. In this problem, a client holds a private string \( \sigma \), a server holds a set of strings \( S \), and the client wants to test whether \( \sigma \in S \) without revealing \( \sigma \) to the server. Unlike in private set intersection [46], the server’s set \( S \) is public. To rule out the trivial solution where the server sends \( S \) to the client, we insist on communication sublinear in \(|S|\). Our approach is approximate: there is some chance that the client outputs “\( \sigma \in S \)” when in fact this is not the case. However, this false-positive rate is bounded even when the set \( S \) and the string \( \sigma \) are chosen adversarially. Looking ahead, our data structure will be at the core of our new scheme for auditing in Certificate Transparence (Section 7).

At a high level, we have the server preprocess its set \( S \) into a data structure. Then, the client, holding a string \( \sigma \), can test whether \( \sigma \in S \) by privately reading a few bits of the server’s data structure using PIR. The relevant cost metrics are:

- **Number of probes.** How many bits of the server’s data structure must the client read?
- **PIR database size.** Over how many bits of the server’s data structure does the client perform its private PIR read?
- **Adversarial false-positive rate.** Given an honest server but an adversarially chosen set \( S \) and string \( \sigma \), what is the probability, only over the client’s secret randomness, that the client outputs “\( \sigma \in S \)” when in fact \( \sigma \notin S \)?

**Background: Bloom filters.** A Bloom filter [15] is a standard data structure for approximate set membership. A one-hash-function Bloom filter consists of a fixed-length bitstring \( D \) and uses a hash function \( H : \{0, 1\}^* \rightarrow \{1, \ldots, |D|\} \). Given a set of strings \( S \subseteq \{0, 1\}^* \), the setup routine hashes each string \( \sigma \in S \) into an index \( i \in \{1, \ldots, |D|\} \) and sets the corresponding bit of the data array: \( D_{H(\sigma)} \leftarrow 1 \). Then, to test whether a string \( \sigma \) is in the set represented by the data structure \( D \), the query algorithm outputs “\( \sigma \in S \)” if and only if the bit \( D_{H(\sigma)} = 1 \).

As long as the query string is chosen independently of the hash function \( H \), the probability of a false-positive is at most \( 1/2 \) when \(|D| \geq 2|S| \). However, when the query string is chosen adversarially—as can be the case in our application—an adversary can easily find strings \( \sigma \in S \) and \( \tilde{\sigma} \notin S \) such that \( H(\sigma) = H(\tilde{\sigma}) \). In this case, the one-hash-function Bloom filter will always incorrectly output “\( \tilde{\sigma} \in S \)” when in fact \( \tilde{\sigma} \in S \). We present a new data structure—which is a twist on Bloom filters—to address this false-positive issue, without increasing the number of probes or the size of the PIR read required by the query algorithm.

**Remark 6.1 (False positives).** Some, but not all, applications can tolerate a non-negligible false-positive rate. For example, credential-breach lookups [66, 82, 91] and contact discovery [60] may tolerate false-positive rates as large as \( 2^{-30} \); in contrast, Safe Browsing blocklist checks [52, 61] demand a cryptographically negligible false-positive rate, as false positives would cause a legitimate website to be flagged as malicious. In the latter case, other data structures may be more appropriate.

6.1 Our approximate membership test

Our data structure for approximate set-membership, illustrated in Figure 4, is parameterized by integers \( a, k \in \mathbb{N} \), a universe of strings \( \mathcal{U} \), and a set size \( N \). The data structure consists of a independent one-hash-function Bloom filters [15], each of size \( kN \) bits. Crucially, these Bloom filters each use independent hash functions, which are chosen after the set \( S \) is fixed. In the remainder of this section, we give an informal description of our construction; a formal treatment appears in Appendix F.

**Data-structure setup.** The setup algorithm takes as input a set of strings \( S \subseteq \mathcal{U} \) of size at most \( N \). The algorithm then chooses a set of \( a \) hash functions—one per Bloom filter—and inserts each string in \( S \) into each of the \( a \) one-hash-function Bloom filters defined by these hash functions. (In practice, we would use a salted hash function with a different salt per filter.)

**Query algorithm.** Given a query string \( \sigma \), the query algorithm chooses an index \( i \leftarrow [a] \) at random, and outputs the result of querying the \( i \)-th one-hash-function Bloom filter on string \( \sigma \).

Our data structure has the following properties:

- **Correctness.** For any set \( S \subseteq \mathcal{U} \) and any query string \( \sigma \in S \), the query algorithm always returns “\( \sigma \in S \).”

- **Adversarial false-positive rate 1/2.** For any set \( S \subseteq \mathcal{U} \) of size at most \( N \), for a random choice of the hash functions used in the data structure, and for any query string \( \tilde{\sigma} \notin S \)—which can depend on the hash functions—the data structure incorrectly returns “\( \tilde{\sigma} \in S \)” with probability at most \( 1/2 \) (taken over the query algorithm’s randomness), for an appropriate choice of the parameters \( a \) and \( k \). In Appendix F, we prove:

**Proposition 6.2:** For all \( \lambda \in \mathbb{N} \), on parameters \( k \geq 8 \) and \( a \geq 2 (\log(|\mathcal{U}|) + \lambda) \), our approximate set-membership data structure has adversarial false-positive rate at most \( 1/2 \). The construction fails with probability \( 2^{-A} \), over the choice of the Bloom filters’ hash functions, modeled as independent random oracles. Concretely, on \(|\mathcal{U}| = 2^{256}\), taking \( a = 768 \) and \( k = 8 \) gives false-positive rate \( 1/2 \) and failure probability \( 2^{-128} \).
**PIR compatibility.** To privately test whether a string is in the set, the client can perform a PIR read over only a small fraction of the data structure. More specifically, the query algorithm probes a single bit in one of the Bloom filters. The client can reveal which Bloom filter it wants to probe to the server, as this does not depend on the query string. So, while the entire data structure consists of \( a kN \) bits, the client can execute a private set-membership test with a PIR read over only \( kN \) bits.

6.2 Related approaches and comparison

We now compare our solution to other data structures for private approximate set-membership, given in Table 5. One natural alternative would be to use a single one-hash-function Bloom filter. (In contrast, our construction uses \( a \approx 768 \) one-hash-function Bloom filters.) However, this approach is not sound in our adversarial setting: as the data structure (including its hash function) is public, an adversary can trivially find a string that causes the query algorithm to always return a false-positive result. We can address this issue by using a Bloom filter with \( O(\lambda) \) hash functions, which gives security against \( 2^{O(\lambda)} \)-time attacks (where \( \lambda = 128 \) is a security parameter). Unfortunately, the query algorithm of such a data structure is roughly \( \lambda N \) more expensive than ours in terms of both (1) the number of probes and (2) the size of the PIR read required for a private query.

Adversarial Bloom filters [28, 45, 78] provide the false-positive guarantees we require, but do not naturally support private reads via PIR. In particular, they have the client send its string \( \sigma \) to the server; the server then applies a pseudorandom function to \( \sigma \) to determine which bits to probe. It is not clear how to use such a data structure in our setting without relatively expensive general-purpose multi-party computation schemes.

Another approach to private set membership has the client and the server execute a PIR by keywords protocol [26]. On security parameter \( \lambda \), the server stores a \( \lambda \)-bit hash of each string in its set in a hash table. Thereafter, the client can perform PIR over this hash table to check if a string is present. While the client probes only few locations of the hash table, its PIR read must cover the entire table, or roughly \( 3.1N \) bits.

Finally, prior work constructs other data structures for approximate set membership [36, 53], offering different performance trade-offs. Combining our ideas for efficiently tolerating false positives in an adversarial setting with such data structures is an intriguing direction for future work.

7 Application: Auditing in Certificate Transparency

We now apply our new PIR schemes (Sections 4 and 5), along with our set-membership data structure (Section 6), to solve the problem of privately auditing signed certificate timestamps in deployments of Certificate Transparency [63, 64, 74].

<table>
<thead>
<tr>
<th></th>
<th>Probes</th>
<th>PIR size</th>
<th>Adv. false-positive rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIR by keywords [26]</td>
<td>2</td>
<td>( 3N )</td>
<td>0</td>
</tr>
<tr>
<td>Standard Bloom filter [15]</td>
<td>( O(\lambda) )</td>
<td>( O(\lambda N) )</td>
<td>0</td>
</tr>
<tr>
<td>1-hash-fn Bloom filter [15]</td>
<td>1</td>
<td>( 2N )</td>
<td>1 (insecure)</td>
</tr>
<tr>
<td><strong>This work</strong></td>
<td>1</td>
<td>( 8N )</td>
<td>1/2</td>
</tr>
</tbody>
</table>

Table 5: Private set-membership data structures, for sets of \( N \) elements from universe \( U \), on security parameter \( \lambda \). The data structures may fail with probability \( k|U| 2^{-A} \), over their random choice of hash functions, modeled as random oracles.

7.1 Problem statement

**Background: Certificate Transparency.** The goal of Certificate Transparency is to store every public-key certificate that every certificate authority issues in a set of publicly accessible logs. To this end, certificate authorities submit the certificates they issue to log operators, who respond with a signed certificate timestamp (SCT). The SCT is a promise to include the new certificate in the log maintained by this operator within some bounded period of time.

Later on, when a TLS server sends a public-key certificate to a client, the server attaches a number of SCTs according to the client’s policy (e.g., Chrome and Safari both require SCTs from three distinct log operators). By verifying the SCTs, the client can be sure that each of the log operators has seen the new certificate and—if the operator is honest—will eventually log it. Domain operators can then use the logs to detect whether a certificate authority has mistakenly or maliciously issued a certificate for their domain. In this setting, the log contents are public; related work investigates scenarios where this is not the case, as in end-user key distribution [75].

**SCT auditing.** To keep the logs honest, some party in the system must verify that the log operators are fulfilling the promise implicit in the SCTs that they issue. In particular, if a client receives an SCT for some certificate \( C \) signed by a log operator, the client would like to verify that \( C \) appears in that operator’s public log. This process is **SCT auditing**.

Clients must be involved in SCT auditing, as they are the only participants who see SCTs “in the wild.” However, the set of SCTs that a client sees reveals information about the client’s browsing history: the fact that a client has seen an SCT for example.com reveals that the client has visited example.com. Thus, to protect its privacy, the client should not reveal which SCTs it has seen to the log operators or to any other entity.

Google’s recent solutions for SCT auditing [35, 89] involve an SCT auditor (run by Google) that is separate from the client. In their model, the auditor maintains the entire set of SCTs for non-expired certificates from all Certificate Transparency logs. Every SCT that a client sees for a live website should appear in the auditor’s set. To determine whether an SCT is valid, a client can check whether it (or really, its SHA256 hash) appears in the set of valid SCTs maintained by the auditor:

- If the client’s SCT appears in the auditor’s set, then the log...
server that issued the SCT correctly fulfilled its promise.

- If not, the client can report the problematic SCT to the auditor to investigate further. Prior work shows how this can be done while keeping the SCT in question hidden [41].

A privacy-protecting solution for SCT auditing must allow the client to test whether its SCT appears in the auditor’s set, without revealing its SCT to the auditor. This is a private set membership problem [91]. While on its surface this problem resembles other applications of PIR in the literature [59, 71], the fact that many clients engage in the protocol with the same auditor means that we can tolerate false positives. That is, it is acceptable for a client to incorrectly believe that an SCT is in the auditor’s set, since over many clients we can expect that missing SCTs are eventually identified. To summarize, we require the following properties, which we state only informally:

- **Correctness with false positives.** When an honest client holding string \( \sigma \), chosen independently of the client’s secret randomness, interacts with an honest auditor holding set \( S \):
  - if \( \sigma \in S \), then the client always outputs “valid,” and
  - if \( \sigma \notin S \), then the client outputs “valid” with probability at most \( 1/2 \), over the choice of the client’s randomness.

- **Privacy for the client.** When an honest client interacts with a malicious auditor, the auditor learns nothing about the client’s private input string \( \sigma \).

  We do not require correctness to hold against a malicious auditor; such an auditor could trivially lie about its set of SCTs.

**System parameters.** There are roughly five billion active SCTs in the web today [35]. Roughly six million of these are added or removed each day as certificate authorities issue certificates and as certificates expire [3]. Google Chrome’s current proposal for SCT auditing has a false-positive rate of essentially zero: when a client audits an SCT, it correctly learns whether the SCT is valid. However, Chrome’s proposal has a detection rate of \( 1/10,000 \): the Chrome client randomly samples \( 0.01\% \) of the SCTs associated with its TLS connections, and audits only this small fraction of all SCTs [2]. This random sampling reduces the amortized cost of auditing by 10,000×, but also reduces the chance that any single auditing client catches a cheating log. Still, across many auditing clients, this randomized SCT auditing catches—with high probability—widely distributed invalid SCTs. After 10,000 clients observe an invalid SCT, in expectation one will audit it and implicate the cheating log.

**Existing approaches.** Two notable proposals for SCT auditing—which do not provide cryptographic privacy—are:

- **Opt-out SCT auditing.** Chrome’s current approach [35] has the client reveal the first 20 bits of the hash of its SCT to the auditor [1]. The auditor replies with all roughly 1000 SCTs in its set that match this 20-bit prefix. This method achieves \( k \)-anonymity for \( k = 1000 \), i.e., it leaks that the client visited one of a set of 1000 sites.

- **Anonymizing proxy.** The client could use proxy servers, such as in Tor [37], to send its SCT to the auditor anonymously [32]; the auditor could reply with the bit indicating whether the SCT appears in its set. This mechanism reveals the entire distribution of clients’ SCTs to the auditor and is susceptible to timing attacks, which could allow the auditor to deanonymize particular clients.

### 7.2 Our approach

We propose a new scheme for SCT auditing that achieves cryptographic privacy. The deployment is as follows:

1. **Auditor: Data-set construction.** The auditor prepares an approximate set-membership data structure holding all SHA256 hashes of all \( N \) active SCTs. This data structure consists of \( a = 768 \) arrays, each \( 8N \) bits in length, and has false-positive rate \( \epsilon = 1/2 \) (Proposition F.1). Then, the auditor runs the PIR Setup routine on each of these \( a \) arrays, producing a PIR hints.

2. **Client: Hint download.** The client chooses a secret, random index \( i^* \in [a] \) and downloads the \( i^* \)-th hint from the auditor, revealing \( i^* \) to the auditor in the process. Whenever the client wants to test whether some SCT appears in the auditor’s set, the client can now read a single bit from the auditor’s \( i^* \)-th array. The probability that a cheating log can trick the client into accepting an invalid SCT is at most \( \epsilon \), the false-positive rate of the underlying set-membership data structure.

   If the client audits an \( f \)-fraction of all of its TLS connections, the detection rate is \( f \cdot (1 - \epsilon) \). In our deployment, we take \( f = 1/5,000 \) and \( \epsilon = 1/2 \). This choice gives an overall detection rate of \( 1/10,000 \)—matching that of Chrome’s current approach [35].

3. **Client and auditor: SCT lookup via PIR.** Each time the client decides to audit an SCT, the client computes the bit of the auditor’s \( i^* \)-th array that it needs to check to verify the SCT’s validity. The client reads this bit privately by running the PIR protocol’s online phase with the auditor, over the \( i^* \)-th array.

   In this approach, the client reuses the same secret index \( i^* \) for multiple SCT lookups. As a result, the events that a client fails to detect invalid SCT A and invalid SCT B are correlated, whereas in Chrome today these events are independent. However, in our approach, the probability that a client catches the first invalid SCT that it looks up remains \( 1 - \epsilon = 1/2 \). As such, the client will catch at least one invalid SCT with probability \( 1/10,000 \) and will thus implicate a cheating log with these odds. Any log that cheats more than 10,000 clients will be caught in expectation.

**Database updates.** In our proposal, the client holds a PIR hint that depends on the auditor’s set of active SCTs. Whenever this set changes, which happens continuously as certificates are issued and expire, the auditor must update its set-membership data structure. Without extra engineering, the client would have to download a fresh PIR hint from the auditor each time.

Our approach has the client download a fresh hint only periodically—one per month, for example. The auditor specifies the range of certificate issue dates that each hint covers. When the client decides to audit an SCT, it checks whether its current hint covers the issue date of the SCT in question. If so,
the client tests the SCT’s validity; if not, the client caches the SCT so as to test its validity the next time it downloads a hint. In this way, the client eventually audits its full random sample of SCTs, but reuses each hint for multiple SCT lookups. The server must now store multiple versions of the database, which is relatively inexpensive; in a large-scale deployment, one or more physical servers could hold each version in memory.

## 8 Evaluation

### Implementation

We implement SimplePIR in fewer than 1,200 lines of Go code, along with 200 lines of C, and DoublePIR in 210 additional lines of Go code. Our code does not rely on any external libraries and is published under the MIT open-source license at github.com/ahenzinger/simplepir. We give sample code for SimplePIR in Appendix G.

We use the appropriate data types to natively support operations over $\mathbb{Z}_q$ (e.g., uint32 for $q = 2^{32}$). We store the database in memory in packed form and decompress it into $\mathbb{Z}_p$ elements on-the-fly, as otherwise the Answer routine is memory-bandwidth-bound. In DoublePIR, we represent the database as a rectangular (rather than square) matrix, so that the first level of PIR dominates the computation.

We run all experiments using a single thread of execution, on an AWS c5n.metal instance running Ubuntu 22.04. To collect the throughput numbers for tables, we run each scheme five times and report the average. All standard deviations in throughput are smaller than 10% of the throughput measured.

### Throughput

In computing the per-server throughput of two-server PIR (from DPFs and from XOR), we divide the measured throughput by two.

### Communication

We run all experiments using a single thread of execution, on an AWS c5n.metal instance running Ubuntu 22.04. To collect the throughput numbers for tables, we run each scheme five times and report the average. All standard deviations in throughput are smaller than 10% of the throughput measured.

### Throughput

In computing the per-server throughput of two-server PIR (from DPFs and from XOR), we divide the measured throughput by two.

### Communication

We run all experiments using a single thread of execution, on an AWS c5n.metal instance running Ubuntu 22.04. To collect the throughput numbers for tables, we run each scheme five times and report the average. All standard deviations in throughput are smaller than 10% of the throughput measured.
communication, amortized over 100 queries, for increasing entry sizes. On databases with short entries, DoublePIR’s amortized communication is comparable to that of the most communication-efficient schemes (Spiral, SpiralPack, SealPIR, and OnionPIR). With larger entries, DoublePIR’s amortized communication costs increase, as the client must download many hints. The two schemes with the closest throughput to ours (SpiralStream and SpiralStreamPack), as well as FastPIR, have much larger amortized communication than both DoublePIR and SimplePIR on entry sizes less than a kilobit.

**Throughput vs. communication trade-off.** We summarize these findings in Figure 6, which displays the throughput/communication trade-off achieved by each PIR scheme. Concretely, we run each scheme on a database of $2^{33}$ bits with increasing entry sizes (as also done in Figure 7). Then, for each scheme, we display the per-query communication (amortized over 100 queries) and the corresponding throughput for two choices of the entry size: one that maximizes the throughput, and another that minimizes the communication. Figure 6 demonstrates that our new PIR schemes achieve a novel point in the design space: SimplePIR and DoublePIR have substantially higher throughput than all prior single-server PIR schemes; DoublePIR further has a per-query communication cost that is competitive with the most communication-efficient schemes.

**Comparison on a database of $2^{33} \times$ 1-bit entries.** In Table 8, we give a fine-grained comparison of the performance of each scheme on a database relevant to our application, consisting of $2^{33}$ 1-bit entries. On this database, SimplePIR and DoublePIR again achieve much higher throughput than all other schemes (9.9 GB/s and 7.4 GB/s respectively). SimplePIR has high offline download and thus also client-side storage costs. However, DoublePIR’s offline download is comparable to the offline communication of other PIR schemes, and its online communication is on the order of kilobytes.

For each scheme, we additionally compute its cost per query, when the client makes 100 queries, using the AWS costs for compute ($1.5 \cdot 10^{-5}$/core-second) and data transfer out of Amazon EC2 ($0.09/GB$). SimplePIR’s per-query cost is $1 \cdot 10^{-4}$, while DoublePIR and the cheapest scheme from related work (SpiralStreamPack) each achieve a per-query cost of $2 \cdot 10^{-5}$. We note, however, that SpiralStreamPack requires megabytes of online upload, which is not reflected in its per-query cost, as AWS only charges for outgoing communication.

**Batching queries.** Finally, we evaluate how SimplePIR and DoublePIR’s effective throughput scales when the client makes a batch of queries for $k$ records at once, assuming the client only needs to recover a constant fraction of the $k$ records. For increasing values of $k$, we compute the expected number of “successful” queries (i.e., the expected number of queries that fall into a distinct database chunk, as discussed in Section 4.3) and we derive the expected “successful” throughput—that is, the throughput measured when the server answers that number of queries at once, with a single pass over the database.

Figure 9 shows that SimplePIR and DoublePIR’s throughput increases when the client makes a batch of queries at once. SimplePIR’s throughput scales linearly, achieving a value of over 100 GB/s on batch size $k \geq 16$ and 1000 GB/s on batch size $k \geq 256$. DoublePIR achieves a throughput over 50 GB/s for $k \geq 32$; when $k \geq 256$, the throughput plateaus at roughly 100 GB/s, as the second level of PIR becomes a bottleneck.

In Appendix H, we give additional benchmarks that measure the server preprocessing time, the client time, and the non-amortized communication of our new PIR schemes, along with tables containing the data displayed in Figures 6, 7 and 9.

### 8.2 Certificate Transparency benchmark

We propose using DoublePIR for the SCT auditing application. With our new data structure for private set membership, the task of SCT auditing requires a single round of PIR over a database with 1-bit entries. For such a database, our microbenchmarks
in Section 8.1 show that DoublePIR achieves both high server throughput and small client storage and communication. SCT auditing occurs in the background, and is not on the critical path to web browsing. Thus, while using PIR may increase the latency of auditing, we believe this is a desirable trade-off in exchange for cryptographic privacy, as long as the computation remains modest and the communication remains comparable.

To benchmark DoublePIR in this application context, we evaluate the scheme on a database consisting of $2^{20}$ × 1-bit entries, which is the size of a Bloom filter in our approximate set membership data structure when we instantiate it with all 5 billion active SCTs. (In our evaluation, each entry is a random bit.) On this database size, we measure that DoublePIR has a “hint” of size 16 MB, an online upload of 724 KB, and an online download of 32 KB. The server can answer each query in fewer than 1.3 core-seconds (and this work is fully parallelizable).

As our client must audit one in every 5,000 TLS connections, our proposal for SCT auditing then requires: (1) 16 MB of client storage and download every month (to keep the client hint), and (2) per TLS connection, an amortized overhead of 0.0003 core-seconds of server compute and 150 bytes of communication. Using the AWS costs for compute ($1.5 \cdot 10^{-5}$ per core second) and data transfer ($0.09$ per outgoing GB), for each client, this amounts to a fixed cost of $0.001$ per month, along with $4 \cdot 10^{-9}$ per TLS connection. For a typical client making $10^4$ TLS connections per week [4], we expect this cost to be roughly $0.02$ per year. Since (after sampling its TLS connections) a typical client makes only few queries to the auditor using each month’s hint, we can reduce the client’s storage to less than 150 KB using the optimization from Appendix E.3.

By comparison, Chrome’s SCT auditing scheme [35] provides only $k$-anonymity for $k = 1,000$: the server learns that a client visited one of a set of 1,000 domains. Auditing incurs an amortized overhead of 24 B of communication per connection\(^2\), negligible server computation, and no client storage (unless the client caches popular SCTs). Again assuming a client making $10^4$ TLS connections per week [4], we expect this scheme to cost roughly $0.001$/client/year. Our approach using DoublePIR incurs $23x$ more communication to achieve the goal of cryptographic privacy.

9 Conclusion

We show that the per-core throughput of single-server PIR can approach the memory bandwidth of the machine and the performance of two-server PIR. Two exciting directions remain open: one is to reduce our schemes’ communication; another is to combine our ideas with those of sublinear-time PIR [30, 31] to reduce the computation beyond the linear-server-time barrier.

\(^2\)The communication may be smaller in practice as the total number of SCTs and the number of SCTs matching each prefix varies.

Acknowledgements. We thank Martin Albrecht for answering questions about LWE hardness estimates, Vadim Lyubashevsky for advice on discrete gaussian sampling, and Adam Belay and Zhenyuan Ruan for discussions about AVX performance. We are grateful to Anish Athalye, Derek Leung, and Ryan Lehmkuhl for reviewing a draft of this work, and to Dima Kogan, David Wu, Jean-Philippe Bossuat, Samir Menon, Alex Davidson, Sofia Celi, Emily Stark, Kevin Yeo, and Joe DeBlasio for helpful conversations and feedback. We thank Sebastian Angel for constructive comments on the discussion of malicious security in an earlier version of this work, and for suggestions on how to improve the presentation. We thank Yuval Ishai and Manto Hamilis for discussing how best to compare against two-server PIR schemes. Yuval also helpfully suggested the “XOR PIR fast” construction discussed in Table 1. This work was supported in part by the National Science Foundation (Award CNS-2054869), a gift from Google, a Facebook Research Award, and MIT’s Fintech@CSAIL Initiative. Alexandra Henzinger was supported by the National Science Foundation Graduate Research Fellowship under Grant No. 2141064 and an EECS Great Educators Fellowship. Matthew M. Hong was funded by NIH R01 HG010959. Vinod Vaikuntanathan was supported by DARPA under Agreement No. HR00112020023, NSF CNS-2154149, MIT-IBM Watson AI, Analog Devices, a Microsoft Trustworthy AI grant and a Thornton Family Faculty Research Innovation Fellowship. 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 the United States Government or DARPA.

References


[4] Mozilla Telemetry Portal, Measurement Dashboard. https://telemetry.mozilla.org/new-pipeline/dist.html#!/cumulative=0&send_date=2022-07-17&include_spill=0&keys=none___!__none___!__none___!__none___!__none___!__none___!__none___!__max_channel_version=nightly%252F104&measure=HTTP TRANSACTION IS SSL&min_channel_version=nightly%252F104&processType= +&product=Firefox&sanitize=1&sort_by_value= 14


Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In *CRYPTO*, 2012.


[91] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh,


[94] Ke Coby Wang and Michael K Reiter. Detecting stuffing A Additional details on related work can learn the contents of all of the client’s PIR queries—even a client’s long-term, secret state. After such an attack, the server can learn the contents of all of the client’s PIR queries—even the ones made before the attacker compromised the server. In

A Additional details on related work

For each PIR scheme from related work, we take its “optimal” entry size to be that for which the highest throughput was reported in the corresponding paper (or, if omitted, in a related paper). For each of our new PIR schemes (SimplePIR and DoublePIR), we compute its “optimal” entry size by executing the scheme on entries of increasing size, and selecting the entry size that yields the highest throughput. In Table 10, we display these entry sizes, along with each PIR scheme’s measured throughput on a database roughly 1 GB in size, with entries of the optimal size.

B Client-state-recovery attacks on some existing PIR schemes

We demonstrate that several recent PIR schemes, including SealPIR and its descendants [6, 8, 9, 76, 77], are insecure against a certain type of active attack that enables the server to recover a client’s long-term, secret state. After such an attack, the server can learn the contents of all of the client’s PIR queries—even the ones made before the attacker compromised the server. In

<table>
<thead>
<tr>
<th>Prior two-server PIR</th>
<th>Database size</th>
<th>Max. achievable throughput/core</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPF PIR [59]</td>
<td>(2^{25})</td>
<td>32 B</td>
</tr>
<tr>
<td>XOR PIR</td>
<td>(2^{33})</td>
<td>1 bit</td>
</tr>
<tr>
<td>XOR PIR fast</td>
<td>(2^{33})</td>
<td>1 bit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prior single-server PIR</th>
<th>Database size</th>
<th>Max. achievable throughput/core</th>
</tr>
</thead>
<tbody>
<tr>
<td>SealPIR [9]</td>
<td>(2^{22})</td>
<td>288 B</td>
</tr>
<tr>
<td>MulPIR [8]</td>
<td>(10^{3})</td>
<td>40 KB</td>
</tr>
<tr>
<td>OnionPIR [77]</td>
<td>(2^{15})</td>
<td>30 KB</td>
</tr>
<tr>
<td>Spiral [76]</td>
<td>(2^{14})</td>
<td>100 KB</td>
</tr>
<tr>
<td>SpiralPack [76]</td>
<td>(2^{15})</td>
<td>30 KB</td>
</tr>
<tr>
<td>SpiralStream [76]</td>
<td>(2^{15})</td>
<td>30 KB</td>
</tr>
<tr>
<td>SpiralStreamPack [76]</td>
<td>(2^{15})</td>
<td>30 KB</td>
</tr>
<tr>
<td>FrodoPIR [34]</td>
<td>(2^{20})</td>
<td>1 KB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>This work (single-server PIR)</th>
<th>Database size</th>
<th>Max. achievable throughput/core</th>
</tr>
</thead>
<tbody>
<tr>
<td>SimplePIR</td>
<td>(2^{20})</td>
<td>1 KB</td>
</tr>
<tr>
<td>DoublePIR</td>
<td>(2^{33})</td>
<td>1 bit</td>
</tr>
</tbody>
</table>

Table 10: Maximal throughput measured for each PIR scheme, on databases of size roughly 1 GB, consisting of \(N\) entries each of size \(d\). The entry sizes, \(d\), are those for which the highest throughput was reported in the corresponding paper. *The throughput is normalized by the number of servers, i.e., divided by two for 2-server PIR schemes. †We estimate MulPIR’s throughput from the measurements given in the paper, as no implementation is publicly available at this date.

contrast, our PIR schemes are not vulnerable to this type of attack (see Remark 3.2) and thus provide a form of forward secrecy (Definition B.1).

Fully reasoning about the security of single-server PIR schemes under active attack is nuanced and beyond the scope of this paper. We point out this active attack to highlight the fact that PIR schemes with secret long-term client state can carry additional security risks that our schemes do not.

The active attack applies to schemes in which the client holds and uses a persistent state across many queries. The state is a secret key for a homomorphic-encryption scheme. In particular, such schemes have the following syntax: first, the client runs a setup algorithm, which we call Setup\(_c\). In contrast, in our new PIR schemes, it is the server who runs the setup algorithm. The Setup\(_c\) algorithm generates two pieces of information:

1. a public hint, \(\sigma_r\), that the client transmits to the server, and
2. a private hint, \(\sigma_e\), that the client keeps to itself.

Both \(\sigma_r\) and \(\sigma_e\) are re-used (by the server and the client respectively) across many queries: each time the client wants to query for some index \(j \in [N]\), the client runs Query\((\sigma_e, j) \rightarrow (st, qu)\) and sends qu to the server. The server runs Answer\((db, \sigma_r, qu) \rightarrow ans\) and sends ans to the client. Finally, the client runs Recover\((st, \sigma_r, ans) \rightarrow d\) to recover the database record of interest. As we will show in the remainder of this section, this syntax can be problematic.
as it lends itself to active attacks in which a malicious server recovers the client’s private, persistent state \( \sigma_c \).

We note that the reason why SealPIR and related schemes reuse a persistent, secret client state over many queries is to save on communication. In these schemes, \( \sigma_c \) holds the client’s secret key for a homomorphic encryption scheme, while \( \sigma_s \) holds some “key-switching hints” associated with this key. The server uses these “key-switching hints” to perform query compression [9] or response packing [6].

**Definition B.1** (Forward secrecy against active attacks). Given a database size \( N \in \mathbb{N} \), a number of queries \( Q \in \mathbb{N} \), and a PIR scheme \( \text{Setup}, \text{Query}, \text{Answer}, \text{Recover} \), consider the following experiment between a challenger and an adversary, 

1. The challenger computes \( (\sigma_s, \sigma_c) \leftarrow \text{Setup}_c(1^4) \) and sends \( \sigma_s \) to the adversary.
2. The adversary sends \( i_0, i_1 \in [N] \) to the challenger.
3. The challenger runs \( \text{Query}(\sigma_c, i_b) \rightarrow (\_ , \text{qu}) \), and sends the query qu to the adversary.
4. For \( q \in \{1, \ldots, Q\} \):
   - The adversary chooses index \( j_q \in [N] \) and sends it to the challenger.
   - The challenger runs \( \text{Query}(\sigma_s, j_q) \rightarrow (\text{st}_q, \text{qu}_q) \) and sends the query \( \text{qu}_q \) to the adversary.
   - The adversary computes some (potentially malformed) \( \text{ans}_q' \), and sends it to the challenger.
   - The challenger runs \( \text{Recover}(\text{st}_q, \sigma_c, \text{ans}_q') \rightarrow d \) and sends it to the adversary. (Note that \( d \) could be the failure symbol, \( \perp \), if the Recover algorithm fails on \( \text{ans}_q' \).)
5. The adversary outputs a guess \( \hat{b} \in \{0, 1\} \).

The PIR scheme satisfies \((T, \epsilon)\)-forward secrecy against active attacks for \( Q \) queries if, for all \( N \in \mathbb{N} \) and all adversaries \( A \) running in time at most \( T \) and making up to \( Q \) queries in the above experiment, it holds that

\[ |\Pr[W_0] - \Pr[W_1]| \leq \epsilon, \]

where \( W_b \) denotes the event that \( A \) outputs “1” in Experiment \( b \), for \( b \in \{0, 1\} \).

**Active attacks on some stateful PIR schemes.** Existing PIR schemes, which let the client reuse a secret key for homomorphic encryption indefinitely, do not provide forward secrecy against active attacks because their underlying homomorphic encryption schemes are not CCA1-secure [25, 43, 44, 70, 96]. In the remainder of this section, we show that there exist attacks that, with polynomially many PIR queries, recover the entire client state. For instance, consider SealPIR with \( d = 1 \) (i.e., no recursion) and recall that the scheme uses BFV encryption [19, 42], where the secret keys are ring elements \( s = s_0 + s_1 x + s_2 x^2 + \cdots + s_{n-1} x^{n-1} \) in the quotient ring \( R_q := \mathbb{Z}_q[x]/(x^n + 1) \) and \( p \) denotes the plaintext modulus. We modify the existing CCA attacks on BFV encryption [25] to obtain Algorithm 1, which is an active attack on SealPIR.

**Conceptually, this attack recovers the client’s secret key by performing a binary search for each \( s_i \in \mathbb{Z}_q \), for \( i \in [n] \).**

**Algorithm 1** Active attack for recovering \( s_i \in \mathbb{Z}_q \) in SealPIR

**Setup**: Let \( O(\cdot) \leftarrow \text{Recover}(st, \sigma_c, \_ ) \). (To implement \( O(\cdot) \) in step 4 of the experiment in Definition B.1, first send \( C \) any index in \([N]\), and then send \( C \) the desired input to \( O(\cdot) \) .) Define \( \Delta \leftarrow [q/p] \).

**Algorithm**: Let \( g \leftarrow O(-1,0), \) where \( g \in \mathbb{Z}_q[x]/(x^n + 1) \). Let \( t \leftarrow g[i] \) (where \( g[i] \) denotes the coefficient of \( x^i \) in \( g \)).

1. If \( t \neq 0 \) then
   - Define \( M \leftarrow \Delta \).
   - Else
     - Define \( M \leftarrow (q \mod p) + \Delta \).

2. Perform binary search to find the smallest \( j \in \{0, 1, \ldots, M\} \) such that \( O(-1, j \cdot x^i)[i] = (t + 1) \mod p \).
3. Output \((t \cdot \Delta + \frac{\Delta}{2}) \mod q \).

**Analysis of Algorithm 1.** In SealPIR, when \( d = 1 \), the client’s private hint \( \sigma_c \) is the BFV secret key, i.e., a secret ring element \( s \in R_q \), that the client uses to generate its queries. The server answers each client query with a single BFV ciphertext \((a, b) \in R_q^2 \). Finally, it holds that

\[ O(-1, j \cdot x^i) = \text{Dec}_{BFV}(s, (-1, j \cdot x^i)) = \text{Round}_\Lambda(j \cdot x^i + s)/\Lambda, \] \hspace{1cm} (1)

where \( \text{Round}_\Lambda(g) \) rounds each coefficient of the polynomial \( g \) to the closest multiple of \( \Lambda := [q/p] \).

By Equation (1), we see that \( t \) (defined as in Algorithm 1) is equal to \( O(-1,0)[i] \), or, equivalently, \( \text{Round}_\Lambda(s_i)/\Lambda \in \mathbb{Z}_p \). Therefore, \( s_i \) must fall into the following ranges:

- If \( t = 0 \), then
  \[ s_i \in \left\{ p \cdot \Delta - \left\lfloor \frac{\Delta}{2} \right\rfloor, \ldots, q - 1 \right\} \cup \left\{ 0, \ldots, \left\lfloor \frac{\Delta}{2} \right\rfloor \right\}. \]

- If \( t \neq 0 \), then
  \[ s_i \in \left\{ t \cdot \Delta - \left\lfloor \frac{\Delta}{2} \right\rfloor, \ldots, t \cdot \Delta + \left\lceil \frac{\Delta}{2} \right\rceil \right\}. \]

Let \( j \) be the smallest value in \([0, \ldots, M]\) such that \( \text{Round}_\Lambda(j + s_i)/\Lambda = \text{Round}_\Lambda(s_i)/\Lambda + 1 \in \mathbb{Z}_p \). The algorithm performs a binary search to find \( j \), requiring roughly \( \log q \) queries to \( O(\cdot) \).

We observe that, after this binary search, \( j \) will be exactly \( T - s_i \), where \( T = t \cdot \Delta + \left\lceil \frac{\Delta}{2} \right\rceil + 1 \) is the “next rounding boundary” of \( \text{Round}_\Lambda(\cdot) \). Finally, the algorithm outputs \( T - j \), which is equal to \( s_i \). Thus, it successfully recovers \( s_i \in \mathbb{Z}_q \), with roughly \( \log q \) queries to \( O(\cdot) \).

To recover the entire secret key \( s \), an attacker can perform the above binary search for all coefficients in \( (s_i)_{i \in [n]} \) in parallel. In other words, instead of asking the oracle \( O \) for \((-1, j \cdot x^i)\), the attacker may ask for \((-1, \sum_{i=1}^n j_i \cdot x^i)\), where the \( \{j_i\}_{i \in [n]} \) are the query points checked by each of the \( n \) parallel binary searches. So, the total number of queries needed to recover \( s \in R_q \) remains roughly \( \log q \). After this attack, the adversary
knows the client’s secret key, \( s \), and can thus learn all of
the client’s past and future PIR queries.

C Additional material on SimplePIR

C.1 Parameter selection

We instantiate SimplePIR with the parameter choices that
maximize its throughput, while meeting the desired correctness
and security requirements. Given a database size \( N \), a correctness
failure probability \( \delta \), an adversary’s runtime \( T \), and a security
failure probability \( \epsilon \), we proceed as follows:

1. We first fix the ciphertext modulus \( q \) to be one of
\( \{2^{16}, 2^{32}, 2^{64}\} \), as modern hardware natively supports oper-
ations over \( \mathbb{Z}_q \) with these moduli.

2. We use LWE hardness estimates \( [7] \) to pick the LWE secret
dimension \( n \) along with the LWE error distribution \( \chi \), such
that a collection of \( \sqrt{N} \) such LWE samples is \( (T, \epsilon) \)-secure
against known attacks.

3. We compute the largest plaintext modulus, \( p \), such that
the chosen LWE parameters support at least \( \sqrt{N} \) homomorphic
additions, with correctness error probability \( \delta \).

In this work, we take \( \chi \) to be a discrete Gaussian distribution.
We give concrete values for our parameters in Section 4.2.

C.2 Correctness and security of SimplePIR

We now give the formal SimplePIR theorem statement:

\[ \text{Theorem C.1 (SimplePIR). On database size } N \in \mathbb{N}, \text{ correctness failure probability } \delta, \text{ adversary runtime } T, \text{ and security failure probability } \epsilon, \text{ let} \]

- \( \chi \) be the discrete Gaussian distribution with variance \( \sigma^2 \),
- \((n, q, \chi)\) be LWE parameters achieving \( (T, \epsilon) \)-security for
\( \sqrt{N} \) LWE samples, and
- \( p \in \mathbb{N} \) be a plaintext modulus chosen to satisfy
\[ [q/p] \geq \sqrt{2} \cdot \sigma \cdot p \cdot N^{1/4} \cdot \sqrt{\ln(2/\delta)}. \]

Then, for a random LWE matrix \( A \in \mathbb{Z}_q^{\sqrt{N} \times N} \), SimplePIR is a
\( (T - O(\sqrt{N}), 2\epsilon) \)-secure PIR scheme on database size \( N \), over
plaintext space \( \mathbb{Z}_p \), with correctness error \( \delta \).

Proof: We prove correctness and security separately.

Correctness. Consider a client that interacts with the server
to query for the database value at \((i_{row}, i_{col}) \in [\sqrt{N}]^2 \). Let
\( u_{i_{row}} \) denote the unit vector \( i_{row} \) in \( \mathbb{Z}_q^{\sqrt{N}} \) (i.e., the vector of all
zeros, with a single ‘1’ at index \( i_{row} \)). The Recover routine in
SimplePIR computes:

\[
\hat{d} = \text{ans}[i_{row}] - \text{hint}_c[i_{row}, \cdot] \cdot s \\
= u^T_{i_{row}} \cdot (\text{ans} - \text{hint}_c, \cdot) \\
= u^T_{i_{row}} \cdot (db \cdot (As + e + \Delta \cdot u_{i_{col}}) - (db \cdot A) \cdot s) \\
= u^T_{i_{row}} \cdot (db \cdot e + \Delta \cdot db \cdot u_{i_{col}}) \\
= db[i_{row}, \cdot] \cdot e + \Delta \cdot db[i_{row}, i_{col}],
\]

where \( db[i_{row}, \cdot] \) denotes row \( i_{row} \) of the database matrix \( db \),
and \( db[i_{row}, i_{col}] \) denotes the element at \((i_{row}, i_{col})\) in \( db \).
Recovery succeeds when \( \text{Round}_A(\hat{d})/\Delta \) is equal to \( db[i_{row}, i_{col}] \).
This happens if and only if \([db[i_{row}, \cdot] \cdot e < \Delta/2\).

We can guarantee successful decryption by ensuring that
\([p/2] \cdot \sqrt{N} \cdot |e|_{\infty} < \Delta/2 \) (because we can store the database
entries—which are elements in \( \mathbb{Z}_p \)—as values in the range
\([-[p/2], -[p/2] + 1, \ldots, [p/2] - 1] \), so that they have maximal norm \([p/2] \)).
However, we instead use a tighter bound on \([db[i_{row}, \cdot] \cdot e] \) by relying on properties of the error
distribution \( \chi \). As a result, we will obtain a scheme in which
decryption succeeds with probability \( 1 - \delta \) (rather than 1) with
a larger plaintext modulus, \( p \).

Indeed, as \( \chi \) is the discrete Gaussian distribution with variance \( \sigma^2 = \frac{s^2}{2\pi} \) for some \( s > 0 \), by \( [68, \text{Lemma 2.2}] [12, \text{Lemma 2.4}] \), for any \( T > 0 \), it holds that,

\[
\Pr \left[ |db[i_{row}, \cdot] \cdot e| \geq T \cdot s \cdot \|db[i_{row}, \cdot]\| \right] < 2 \exp(-\pi \cdot T^2),
\]

where \( \| \cdot \| \) denotes the Euclidean norm.
Taking \( T = \Delta/(2s \cdot \|db[i_{row}, \cdot]\|) \), we see that

\[
\Pr \left[ |db[i_{row}, \cdot] \cdot e| \geq \Delta/2 \right] < \delta,
\]

as long as

\[
2 \exp \left(-\pi \cdot \left(\frac{\Delta}{2s \cdot \|db[i_{row}, \cdot]\|}\right)^2\right) \leq \delta.
\]

Equivalently, recovery fails with probability at most \( \delta \), if
\[
\Delta \geq 2s \cdot \|db[i_{row}, \cdot]\| \cdot \sqrt{\frac{\ln(2/\delta)}{\pi}}.
\]

Again, as we can store the elements in \( db \) in the range
\([-[p/2], [p/2]]\), we have that

\[
\|db[i_{row}, \cdot]\| \leq \sqrt{\sqrt{N} \cdot \frac{[p/2]^2}{\pi}} = N^{1/4} \cdot \frac{[p/2]}{\pi}.
\]

In addition, we know that \( \Delta = \lfloor q/p \rfloor \) and \( s = \sigma \cdot \sqrt{2\pi} \). Thus,
recovery fails with probability at most \( \delta \), as long as:

\[
\lfloor q/p \rfloor \geq \sigma \cdot \sqrt{2\pi} \cdot p \cdot N^{1/4} \cdot \sqrt{\frac{\ln(2/\delta)}{\pi}},
\]
or, equivalently,

\[
\lfloor q/p \rfloor \geq \sqrt{2} \cdot \sigma \cdot p \cdot N^{1/4} \cdot \sqrt{\ln(2/\delta)},
\]
By Equation (2), this condition holds. Thus, SimplePIR is correct, except with error probability at most \( \delta \).

**Security.** Security follows from the fact that the LWE problem is hard, even when the LWE matrix \( \mathbf{A} \) is reused across many independent trials, each using an independently generated LWE secret \( s \leftarrow \mathbb{Z}_q\), as shown in prior work \cite[Lemma 7.3]{83}.

We connect the security of SimplePIR to the hardness of LWE with the following lemma:

**Lemma C.2.** Let \( N \in \mathbb{N} \) be the database size, \((n,q,\chi)\) be the LWE parameters, and \( \mathbf{A} \in \mathbb{Z}_q^{\sqrt{N} \times n} \) be the random LWE matrix used in SimplePIR. For any \( i \in [N] \), we define the distribution \( Q_i = \{(\mathbf{A}, qu_i) : \_qu_i \leftarrow \text{Query}(i)\} \).

If the \((n,q,\chi)\)-LWE problem with \( \sqrt{N} \) samples is \((T,\epsilon)\)-hard, then any algorithm running in time \( T - O(\sqrt{N}) \) can have success probability at most \( \epsilon \) in distinguishing \( Q_i \) from the distribution \( \{(\mathbf{A}, r) : r \leftarrow \mathbb{Z}_q^{\sqrt{N}}\} \).

**Proof.** Consider any index \( i \in [N] \). We decompose \( i \) into the pair of coordinates \((i_{\text{row}},i_{\text{col}}) \in [\sqrt{N}]^2 \), as done in the Query routine in SimplePIR, and let \( u_{\text{col}} \) denote unit vector \( i_{\text{col}} \) in \( \mathbb{Z}_q^{\sqrt{N}} \). Additionally, we define the following distributions:

- \( D_1 = \{(\mathbf{A}, \mathbf{s} + \mathbf{e}) : \mathbf{e} \leftarrow \mathbb{Z}_q^{\sqrt{N}} \} \); and
- \( D_2 = \{(\mathbf{A}, r) : r \leftarrow \mathbb{Z}_q^{\sqrt{N}}\} \).

Now, consider the simulator \( S \) that, given as input \((\mathbf{A}, \mathbf{v}) \in \mathbb{Z}_q^{\sqrt{N} \times n} \times \mathbb{Z}_q^{\sqrt{N}}\), computes and outputs \((\mathbf{A}, \mathbf{v} + [q/p] \cdot u_{\text{col}}) \).

We observe that:

- when \((\mathbf{A}, \mathbf{v})\) is sampled from \( D_1 \), the simulator’s output is distributed identically to \( Q_i \).
- when \((\mathbf{A}, \mathbf{v})\) is sampled from \( D_2 \), the simulator’s output is distributed identically to \( D_2 \).

As the \((n,q,\chi)\)-LWE problem with \( \sqrt{N} \) samples is \((T,\epsilon)\)-hard, we know that any algorithm running in time \( T \) has advantage at most \( \epsilon \) in distinguishing between \( D_1 \) and \( D_2 \). Our simulator \( S \) runs in time \( O(\sqrt{N}) \). Thus, it must hold that any algorithm distinguishing between \( Q_i \) and \( D_2 \) in time at most \( T - O(\sqrt{N}) \) can have success probability at most \( \epsilon \). \( \square \)

**Corollary C.3** \((Q\text{-query security of SimplePIR}). \) For any sequence \( I \in [N]^Q \) of \( Q \) indices, we define \( \mathcal{D}_I \) to be the query distribution that it induces, i.e.,

\[
\mathcal{D}_I = \{(\mathbf{A}, qu_k) : qu_k \leftarrow \text{Query}(I_k)\}_{k \in [Q]}
\]

Also, we define the random query distribution, \( \mathcal{R} \):

\[
\mathcal{R} = \{(\mathbf{A}, r) : r \leftarrow \mathbb{Z}_q^{\sqrt{N}}\}_{k \in [Q]}
\]

If the \((n,q,\chi)\)-LWE problem with \( \sqrt{N} \) samples is \((T,\epsilon)\)-hard, then \( \mathcal{D}_I \) is \((T - O(Qn\sqrt{N}),\epsilon)\)-indistinguishable from \( \mathcal{R} \).

**Proof.** The proof follows by a standard hybrid argument. Let \( I \in [N]^Q \) be a sequence of \( Q \) indices. For any \( j \in [Q] \), we define the hybrid distribution, \( H_j \):

\[
H_j = \{(\mathbf{A}, r) : r \leftarrow \mathbb{Z}_q^{\sqrt{N}}\}_{k \in [j,\ldots,j]}
\cup \{(\mathbf{A}, qu_k) : qu_k \leftarrow \text{Query}(I_k)\}_{k \in (j+1,\ldots,Q)}.
\]

In other words, \( H_j \) is the distribution where the first \( j \) queries are truly random vectors, and the remaining \((Q - j)\) queries are sampled from \( \mathcal{D}_I \). As such, \( H_0 = \mathcal{D}_I, \) while \( H_Q = \mathcal{R} \).

Now, consider any algorithm \( A \) that runs in time \( t \) and distinguishes between distributions \( H_0 \) and \( H_Q \) with advantage at least \( p \). For any \( j \in [Q] \), we define \( p_j \) to be the probability that \( A \) outputs 1 when given samples from \( H_j \). By definition,

\[
p = |p_Q - p_0| = \sum_{j=1}^{Q} (p_j - p_{j-1})
\]

Thus, there exists some \( j^* \) in \([Q]\) such that

\[
|p_{j^*} - p_{j^*-1}| \geq p/Q.
\]

Using \( A \) as a subroutine, we then build an algorithm \( B \) that distinguishes between the distributions \( \mathcal{Q}_{I_{j^*}} \) (defined in Lemma C.2) and \( \{(\mathbf{A}, r) : r \leftarrow \mathbb{Z}_q^{\sqrt{N}}\} \).

**Algorithm 2** \( B \), on input \((\mathbf{A}, b)\):

```
for \( j = 1,\ldots,j^* - 1 \) do
    Compute \( r_j \leftarrow \mathbb{Z}_q^{\sqrt{N}} \)
end for
for \( j = j^* + 1,\ldots,Q \) do
    Compute \( qu_j \leftarrow \text{Query}(I_j) \)
end for
Output
\[ A\left((\mathbf{A}, r_1),\ldots,(\mathbf{A}, r_{j^*-1}), (\mathbf{A}, b), (\mathbf{A}, qu_{j+1}),\ldots,(\mathbf{A}, qu_Q)\right) \]
```

Then, we observe that:

- When \( B \) is given an input sampled from \( \mathcal{Q}_{I_{j^*}} \), the input that \( B \) feeds to \( A \) is distributed following \( H_{j^*} \). As such, \( B \) outputs 1 with probability \( p_{j^*} \).
• When \( B \) is given an input sampled from \( \left\{ (A, r) : r \sim \mathbb{Z}_q^N \right\} \), the input that \( B \) feeds to \( A \) is distributed following \( H_{j+1} \). As such, \( B \) outputs 1 with probability \( p_{j+1} \).

So, \( B \) distinguishes between the distributions \( Q_{t_j} \), and \( \left\{ (A, r) : r \sim \mathbb{Z}_q^N \right\} \) with advantage at least \( |p_{j'} - p_{j-1}| \geq p/Q \). Further, \( B \) runs in time \( t + O(Qn\sqrt{N}) \), as \( Q \) takes time \( O(n\sqrt{N}) \).

By Lemma C.2, we conclude that, if the \( (n, q, \chi) \)-LWE problem with \( \sqrt{N} \) samples is \((T, \varepsilon)\)-hard and \( t + O(Qn\sqrt{N}) \leq T - O(\sqrt{N}) \), it must hold that \( p/Q < \varepsilon \). In other words, if the \( (n, q, \chi) \)-LWE problem with \( \sqrt{N} \) samples is \((T, \varepsilon)\)-hard, then \( D_t \) is \((O(T - Qn\sqrt{N}), Q\varepsilon)\)-indistinguishable from \( R \). □

C.3 Additional extensions and optimizations

Answering many client queries at once. To answer \( n \) client queries simultaneously by the server, the client needs to encrypt in the ciphertext space, \( \mathbb{Z}_q \), \( m \) queries and must be updated. In other words, it is sufficient for the server to compute \( m \) · \( \text{hint}_c \) to be the product of the database matrix, \( \mathbf{db} \), the LWE matrix, \( \mathbf{A} \). Thus, when some row \( \mathbf{d} \) of the database changes, only the corresponding row in \( \text{hint}_c \) changes and must be updated. In other words, it is sufficient for the server to compute \( m \) · \( \mathbf{A} \in \mathbb{Z}_q^{n \times n} \) (rather than the much more expensive \( \mathbf{db} \cdot \mathbf{A} \in \mathbb{Z}_q^{n \times n} \)) and send it back to the client. Additions and deletions of rows in \( \mathbf{db} \) can be handled similarly.

Decreasing the online download with local rounding. In SimplePIR’s online phase, the client downloads a vector of \( \sqrt{N} \) elements in the ciphertext space, \( \mathbb{Z}_q \), performs a linear computation on them, and finally rounds the result to map it into the message space, \( Z_p \). Prior work [38, Lemma 3.2][39, Lemma 4.1][18, Lemma 1] observes that, for any value \( v \in \mathbb{Z}_q \) that is “close” to a multiple of \( \Delta \), and for a random \( r \in \mathbb{Z}_q \), it holds with high probability that

\[
\text{Round}_\Delta(v) = \text{Round}_\Delta(v + r) - \text{Round}_\Delta(r).
\]

Using this observation (with \( v \leftarrow \text{ans} - \text{hint}_c \cdot s \) and \( r \leftarrow \text{hint}_c \cdot s \)), the server and the client could each locally round the values they contribute to the client’s final computation (ans and \( \text{hint}_c \cdot s \), respectively), decreasing the online download to only \( \sqrt{V} \) elements in \( Z_p \). If the LWE parameters are chosen appropriately (namely, \( [q/p] \geq \sqrt{2 \cdot \frac{4}{3} \cdot \sigma \cdot p \cdot N^{1/4} \cdot \sqrt{\ln(8/\delta)}} \)), then this local rounding does not affect the scheme’s correctness (i.e., recovery still succeeds, except with probability \( \delta \)).

In practice, this optimization decreases the online download by a factor of \( \log q / \log p \approx 3 \times \), at the expense of requiring a much smaller plaintext modulus, \( p \), to maintain correctness and thus markedly reducing SimplePIR’s throughput. Exploring other approaches to local rounding [20] or to correcting the errors that it introduces are interesting directions for future work.

D Linearly homomorphic encryption with preprocessing

In this section, we abstract out the key property of Regev encryption that enables SimplePIR’s high throughput. We expect this primitive to have applications beyond PIR.

Specifically, we introduce the notion of \textit{linearly homomorphic encryption with preprocessing}. This notion is similar to standard linearly homomorphic encryption: given an encryption of vector \( v \in \mathbb{Z}_p^m \) (where the ring \( \mathbb{Z}_p \) and dimension \( m \) are parameters of the scheme), it is possible to homomorphically evaluate any linear function \( f : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p \) on the encrypted values; after evaluation, the resulting ciphertext decrypts to the function value \( f(v) \). What distinguishes our use of Regev encryption from standard linearly homomorphic encryption is that we can precompute the function \( f \) to speed up the homomorphic-evaluation operation. In particular, given a linear function \( f \), we compute a preprocessed hint, \( \text{hint}_f \).

The hint enables homomorphic evaluation of \( f \) on ciphertexts encrypting any \( v \in \mathbb{Z}_p^m \) at very low computational cost—nearly the cost of evaluating \( f \) on a plaintext vector.

D.1 Definition

Formally, a \textit{linearly homomorphic encryption scheme with preprocessing} consists of the following efficient algorithms, which are implicitly parameterized by a security parameter \( n \in \mathbb{N} \), a correctness parameter \( \delta \in \mathbb{N} \), a plaintext dimension \( m \in \mathbb{N} \), a key space \( \mathcal{K} \), and a plaintext space \( \mathbb{Z}_p \):

\begin{align*}
\text{Setup}() & \rightarrow \mathbf{pp}. \text{Sample and output the public parameters.} \\
\text{Enc}(\mathbf{pp}, \mathbf{sk}, v) & \rightarrow \mathbf{ct}. \text{Given the public parameters \( \mathbf{pp} \), a secret key \( \mathbf{sk} \in \mathcal{K} \), and a vector \( v \in \mathbb{Z}_p^m \), output a ciphertext \( \mathbf{ct} \).} \\
\text{Preproc}(\mathbf{pp}, f) & \rightarrow \text{hint}_f. \text{Given public parameters \( \mathbf{pp} \) and a linear function \( f : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p \), output a function hint \( \text{hint}_f \).}
\end{align*}
Apply(pp, f, ct) → ct_f. Given the public parameters pp, a linear function f : Z_p^m → Z_p, and a ciphertext ct, produce a ciphertext ct_f that encrypts the value of the function f applied to the vector encrypted by ct.

Dec(sk, hint_f, ct_f) → d. Given a secret key sk, the function hint hint_f, and a ciphertext ct_f, output a decrypted value d.

Correctness. After encryption, preprocessing and application of the linear function, and decryption are carried out sequentially, the output should be the correct function value, except with negligible probability in the implicit correctness parameter. Formally, we say that the encryption scheme has correctness error δ if, for all sk ∈ K, for all v ∈ Z_p^m, and linear functions f ∈ Z_p → Z_p, the following probability is at least 1 − δ:

\[
\Pr \left[ d = f(v) : \text{hint}_f \leftarrow \text{Preproc}(pp, f), c_t \leftarrow \text{Apply}(pp, f, c_t), d \leftarrow \text{Dec}(sk, \text{hint}_f, c_t) \right] \leq \delta
\]

Security. We require semantic security [51]. In other words, ct should reveal no information about the encrypted vector v = (v_1, ..., v_m). Formally, given vectors v_0, v_1 ∈ Z_p^m, for b ∈ {0, 1}, we define the value W_b as:

\[
W_b := \Pr \left[ A(pp, ct) = 1 : \begin{array}{l}
pp \leftarrow \text{Setup}() \\
ct \leftarrow \text{Enc}(pp, sk, v_b) \\
\end{array} \right]
\]

Then, we say that the encryption scheme is secure if, for all efficient adversaries A, for all v_0, v_1 ∈ Z_p^m, it holds that |W_0 − W_1| is negligible in the implicit security parameter.

D.2 Construction

In Figure 12, we construct a linear homomorphic encryption scheme with preprocessing from Regev encryption. The construction yields the following theorem:

Theorem D.1. Assume the (n, q, χ)-LWE problem with m samples is (T, ϵ)-hard, and let p ∈ N be a suitable plaintext modulus\(^3\) for Regev encryption with these parameters supporting m homomorphic additions. Then, the construction of Figure 12 is a (T − O(m), 2ε)-secure linearly homomorphic encryption scheme with preprocessing for plaintext dimension m and plaintext modulus p where:

- the hint consists of n elements of Z_q,
- the ciphertext encrypting a vector in Z_p^m consists of m elements of Z_q,
- the evaluation routine Apply requires m additions and m multiplications in Z_q, and
- the ciphertext that Apply outputs consists of one Z_q element.

\(^3\)To support arbitrary linear functions, it is necessary to take p \mid q. To support linear functions whose output will not wrap around \mod p (as is the case for PIR), such a restriction on p is not necessary.

It is worth emphasizing the efficiency of the construction implied by Theorem D.1. By our choice of LWE parameters in Equation (2), the number of bits encoding each ciphertext element (i.e., \log q) grows logarithmically with the plaintext dimension m and is independent of the security parameter n. Thus, our construction has:

- a hint size that grows only logarithmically with the size of the linear function f,
- ciphertext size that is only a log m factor larger than the corresponding plaintext (and that is independent of the security parameter), and
- a homomorphic evaluation routine that is essentially as fast as plaintext evaluation of f, as homomorphic evaluation just requires computing f over Z_q instead of over Z_p. This evaluation time is independent of the security parameter.

In contrast, when using Paillier [81] or ElGamal-based [40] linearly homomorphic encryption, the ciphertext size and evaluation time grow quadratically or cubically with the security parameter (Table 11).

D.3 Abstract view of SimplePIR

In Figure 13, we re-express the SimplePIR construction of Section 4 in the language of linear homomorphic encryption with preprocessing. The PIR scheme of Figure 13 demonstrates that, given a linearly homomorphic encryption scheme with preprocessing, there exists a PIR scheme with \sqrt{N} communication cost and for which the server’s online computation time consists of running the encryption’s Apply algorithm \sqrt{N} times, each on a vector of dimension \sqrt{N}. The client’s hint—which it must fetch in an offline phase—consists of \sqrt{N} hints for the encryption scheme, each computed for a linear function with \sqrt{N} inputs.

An interesting task for future work would be to construct a linear homomorphic encryption scheme with preprocessing with smaller hints. This would reduce the offline communication in the resulting PIR schemes.

<table>
<thead>
<tr>
<th>Size</th>
<th>Running time (per bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hint</td>
<td>Key</td>
</tr>
<tr>
<td>Factoring [79, 81]</td>
<td>n/a</td>
</tr>
<tr>
<td>EC ElGamal [40]</td>
<td>n/a</td>
</tr>
<tr>
<td>Regev [83, 86]</td>
<td>n/a</td>
</tr>
<tr>
<td>Ring LWE [72]</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>This work</strong> (LWE)</td>
<td>λ</td>
</tr>
</tbody>
</table>

Table 11: Comparison of linearly homomorphic encryption schemes on plaintext dimension m. We suppress \log λ factors and we assume that it is possible to perform modular multiplication in linear time. Since our scheme uses plain LWE instead of ring LWE, it is simpler to implement—there is no need for polynomial arithmetic, fast Fourier transforms, or a modulus of special form.
We detail our calculation of \( \Delta := \lfloor q/p \rfloor \). The keyspace is \( \mathcal{K} = \mathbb{Z}_q^n \).

\[
\text{Setup}(\cdot) \rightarrow pp \in \mathbb{Z}_q^{m \times n}
\]
- Sample \( A \leftarrow \mathbb{Z}_q^{m \times n} \).
- Return \( pp \leftarrow A \).

\[
\text{Enc}(pp, sk, v) \rightarrow ct \in \mathbb{Z}_q^m
\]
- Parse \( (A \in \mathbb{Z}_q^{m \times n}) \leftarrow pp \).
- Sample \( e \leftarrow \mathbb{Z}_q^m \).
- Return \( ct \leftarrow A \cdot sk + e + \Delta \cdot v \in \mathbb{Z}_q^m \).

\[
\text{Preproc}(pp, f) \rightarrow \text{hint}_f \in \mathbb{Z}_q^{1 \times n}
\]
- Parse \( (A \in \mathbb{Z}_q^{m \times n}) \leftarrow pp \).
- Parse \( (f \in \mathbb{Z}_q^{1 \times m}) \leftarrow f \) as a row vector.
- Return \( \text{hint}_f \leftarrow f \cdot A \).

\[
\text{Apply}(pp, f, ct) \rightarrow ct_f \in \mathbb{Z}_q
\]
- Parse:
  - \( (f \in \mathbb{Z}_q^{1 \times m}) \leftarrow f \) as a row vector,
  - \( (c \in \mathbb{Z}_q^m) \leftarrow ct \).
- Return \( ct_f \leftarrow f \cdot c \in \mathbb{Z}_q \).

\[
\text{Dec}(pp, sk, \text{hint}_f, ct_f) \rightarrow d \in \mathbb{Z}_p
\]
- Compute \( \hat{d} \leftarrow ct_f - \text{hint}_f \cdot sk \in \mathbb{Z}_q \).
- Let \( v \in \mathbb{Z}_q \) be \( \text{Round}_\Delta(\hat{d}) \), which is \( \hat{d} \) rounded to the nearest integral multiple of \( \Delta \).
- Return \( d \leftarrow v/\Delta \in \mathbb{Z}_p \).

\[\text{Parameters:} \text{LWE parameters } (n, q, \chi), \text{a plaintext modulus } p < q. \text{Define } \Delta := \lfloor q/p \rfloor. \text{The keyspace is } \mathcal{K} = \mathbb{Z}_q^n.\]

\[\text{Setup}(\cdot) \rightarrow pp \in \mathbb{Z}_q^{m \times n}\]
- Sample \( A \leftarrow \mathbb{Z}_q^{m \times n} \).
- Return \( pp \leftarrow A \).

\[\text{Enc}(pp, sk, v) \rightarrow ct \in \mathbb{Z}_q^m\]
- Parse \( (A \in \mathbb{Z}_q^{m \times n}) \leftarrow pp \).
- Sample \( e \leftarrow \mathbb{Z}_q^m \).
- Return \( ct \leftarrow A \cdot sk + e + \Delta \cdot v \in \mathbb{Z}_q^m \).

\[\text{Preproc}(pp, f) \rightarrow \text{hint}_f \in \mathbb{Z}_q^{1 \times n}\]
- Parse \( (A \in \mathbb{Z}_q^{m \times n}) \leftarrow pp \).
- Parse \( (f \in \mathbb{Z}_q^{1 \times m}) \leftarrow f \) as a row vector.
- Return \( \text{hint}_f \leftarrow f \cdot A \).

\[\text{Apply}(pp, f, ct) \rightarrow ct_f \in \mathbb{Z}_q\]
- Parse:
  - \( (f \in \mathbb{Z}_q^{1 \times m}) \leftarrow f \) as a row vector,
  - \( (c \in \mathbb{Z}_q^m) \leftarrow ct \).
- Return \( ct_f \leftarrow f \cdot c \in \mathbb{Z}_q \).

\[\text{Dec}(pp, sk, \text{hint}_f, ct_f) \rightarrow d \in \mathbb{Z}_p\]
- Compute \( \hat{d} \leftarrow ct_f - \text{hint}_f \cdot sk \in \mathbb{Z}_q \).
- Let \( v \in \mathbb{Z}_q \) be \( \text{Round}_\Delta(\hat{d}) \), which is \( \hat{d} \) rounded to the nearest integral multiple of \( \Delta \).
- Return \( d \leftarrow v/\Delta \in \mathbb{Z}_p \).
Construction: DoublePIR. The parameters of the construction are a database size $N$, database dimensions $\ell$ and $m$ (such that $\ell \cdot m \geq N$), LWE parameters $(n, q, \chi)$, plaintext modulus $p < q$, and LWE matrices $A_1 \in \mathbb{Z}_q^{m \times n}$ and $A_2 \in \mathbb{Z}_q^{\ell \times n}$ (sampled in practice using a hash function). The database consists of $N$ values in $\mathbb{Z}_p$, represented as a matrix in $\mathbb{Z}_p^{\ell \times m}$. We define the scalars $\kappa := \left\lceil \frac{\log q}{\log p} \right\rceil$ and $\Delta := \left\lceil \frac{q}{p} \right\rceil$. We use the helper routines:

- **Decomp**: $\mathbb{Z}_q^{\ell \times m} \rightarrow \mathbb{Z}_q^{\ell \times \ell}$, which writes each $\mathbb{Z}_q$ element as its base-$p$ decomposition,
- **Recomp**: $\mathbb{Z}_q^{\ell \times m} \rightarrow \mathbb{Z}_q^{\ell \times \ell}$, which interprets each $\kappa \times 1$ submatrix of its input as a base-$p$ decomposition of a $\mathbb{Z}_q$ element and outputs the matrix of these elements,
- Round$_{\Delta}$: $\mathbb{Z}_q^a \rightarrow \mathbb{Z}_q^a$, which rounds each entry to the nearest integral multiple of $\Delta$.

\[
\text{Setup}(db \in \mathbb{Z}_p^{\ell \times m}) \rightarrow (\text{hint}_t, \text{hint}_c).
\]

- **Compute** \[
\begin{align*}
\text{hint}_t & \leftarrow \text{Decomp}(A_1 \cdot db^T) \in \mathbb{Z}_q^{\ell \times \ell} \\
\text{hint}_c & \leftarrow \text{hint}_t \cdot A_2 \in \mathbb{Z}_q^{\ell \times n} \\
\text{return} \ (\text{hint}_t, \text{hint}_c)
\end{align*}
\]

- **Query** $(i \in [N]) \rightarrow (st, qu)$,

\[
\begin{align*}
\text{Write} \ i \ as \ a \ pair \ (i_{\text{row}}, i_{\text{col}}) \in [\ell] \times [m]. \\
\text{Sample} \ s_1 \ \& \ s_2 \ \in \mathbb{Z}_q^m, \\
\text{such that} \ s_1 \ \& \ s_2 \ \in \mathbb{Z}_q^m. \\
\text{Compute} \ c_1 \leftarrow (A_1 \cdot s_1 + e_1 + \Delta \cdot u_{i_{\text{col}}}) \in \mathbb{Z}_q^m, \\
\text{c}_2 \leftarrow (A_2 \cdot s_2 + e_2 + \Delta \cdot u_{i_{\text{row}}}) \in \mathbb{Z}_q^\ell, \\
\text{where} \ u_i \ \text{is the vector of all zeros with a single} \ '1' \ \text{at index} \ i. \\
\text{Return} \ (st, qu) \leftarrow ((s_1, s_2), (c_1, c_2)).
\end{align*}
\]

Answer($db, \text{hint}_t, \text{qu}) \rightarrow \text{ans}.

- **Parse** $(c_1 \in \mathbb{Z}_q^m, c_2 \in \mathbb{Z}_q^\ell) \leftarrow \text{qu}.
\begin{align*}
\text{ans}_1 & \leftarrow \text{Decomp}(c_1^T \cdot db^T) \in \mathbb{Z}_q^{\ell \times \ell} \\
\text{h} & \leftarrow \text{ans}_1 \cdot A_2 \in \mathbb{Z}_q^{\ell \times n}, \\
\text{Compute} \ \begin{pmatrix} \text{ans}_0 \\ \text{ans}_1 \\ \text{ans}_2 \end{pmatrix} \leftarrow \begin{pmatrix} \text{hint}_t \\ \text{ans}_1 \\ \text{ans}_1 \end{pmatrix} \cdot \begin{pmatrix} e_1 \\ e_2 \\ 1 \end{pmatrix} \in \mathbb{Z}_q^{k(n+1)}.
\end{align*}

- Return $\text{ans} \leftarrow (h, \text{ans}_0, \text{ans}_2)$.

Recover($st, \text{hint}_c, \text{ans}) \rightarrow d.$

- **Parse**:\n
  \[
  \begin{pmatrix} s_1 \in \mathbb{Z}_q^n, s_2 \in \mathbb{Z}_q^n \end{pmatrix} \leftarrow \text{st},
  \begin{pmatrix} h \in \mathbb{Z}_q^{k \times n}, \text{ans}_1 \in \mathbb{Z}_q^{k \times n}, \text{ans}_2 \in \mathbb{Z}_q^n \end{pmatrix} \leftarrow \text{ans}.
  \]

- **Compute**:\n
  \[
  \begin{pmatrix} \hat{h}_1 \\ \text{ans}_1 \\ \text{ans}_2 \end{pmatrix} \leftarrow \begin{pmatrix} \text{hint}_c \\ h \end{pmatrix} \cdot \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \in \mathbb{Z}_q^{k \times (n+1)},
  \]

  \[
  \begin{pmatrix} \hat{d} \\ \text{ans}_1 \end{pmatrix} \leftarrow \text{Recomp} \left( \text{Round}_\Delta \left( \frac{\hat{h}_1}{\text{ans}_1} \right) / \Delta \right) \in \mathbb{Z}_q^{n+1},
  \]

  \[
  d \leftarrow \text{ans}_1 - 2^h \cdot \hat{d} \in \mathbb{Z}_q.
  \]

- Return $d \leftarrow \text{Round}_\Delta (\hat{d}) / \Delta \in \mathbb{Z}_p$.

Figure 14: The DoublePIR protocol.

E.2 Correctness and security of DoublePIR

We now prove the following theorem:

**Theorem E.1** (DoublePIR). On database size $N \in \mathbb{N}$, correctness failure probability $\delta$, adversary runtime $T$, and security failure probability $\epsilon$, let

- $\ell, m \in \mathbb{N}$ be database dimensions (such that $\ell \cdot m \geq N$),
- $\chi$ be the discrete Gaussian distribution with variance $\sigma^2$,
- $(n, q, \chi)$ be LWE parameters achieving $(T, \epsilon)$-security for max($\ell, m$) LWE samples, and
- $p \in \mathbb{N}$ be a plaintext modulus chosen to satisfy

\[
\left\lceil \frac{q}{p} \right\rceil \geq \sigma \sqrt{2 \max(m, \ell) \cdot \ln \left(\frac{2(k(n+1)+1)}{\delta}\right)}, \tag{3}
\]

where $k \in \mathbb{Z}$ is the scalar $\left\lceil \frac{\log q}{\log p} \right\rceil$.

Then, for random LWE matrices $A_1 \leftarrow \mathbb{Z}_q^{m \times n}$ and $A_2 \leftarrow \mathbb{Z}_q^{\ell \times n}$, DoublePIR is a $(T - O(n \cdot k + m), 4\epsilon)$-secure PIR scheme on database size $N$, over plaintext space $\mathbb{Z}_p$, with correctness error $\delta$.

**Proof.** We prove correctness and security separately.

**Correctness.** Consider a client that queries for the database value at index $(i_{\text{row}}, i_{\text{col}}) \in [\ell] \times [m]$. We observe that the Recover routine in DoublePIR essentially runs $k \cdot (n + 1) + 1$ instances of SimplePIR’s recovery routine, to recover $k \cdot (n + 1) + 1$ elements in $\mathbb{Z}_p$, namely:

- one $\mathbb{Z}_p$-element that encodes the database value at index $(i_{\text{row}}, i_{\text{col}})$ (in the “first level of PIR”),
- $k\Delta$ additional $\mathbb{Z}_p$-elements that encode the $\Delta \mathbb{Z}_p$-elements
in row \( i_{\text{row}} \) of the first-level hint matrix, \( A_i^T \cdot \text{db}^T \) (in the “second level of PIR”), and
• \( \kappa \) additional \( \mathbb{Z}_q^\kappa \)-elements that encode the single \( \mathbb{Z}_q \)-element at position \( i_{\text{row}} \) in the first level answer vector, \( e_1^T \cdot \text{db}^T \) (in the “second level of PIR”).

For the recovery to succeed, all \( \kappa \cdot (n + 1) + 1 \) invocations of SimplePIR’s recovery must succeed. To bound this probability, we compute the probabilities of two separate events:

• \( E_1 \), the event that the recovery of the \( \kappa \cdot (n + 1) \) elements in the “second level of PIR” fails, i.e., that

\[
\begin{bmatrix}
\hat{h}_i \\
a_1
\end{bmatrix} \neq \text{Recomp} \left( \begin{bmatrix}
\text{hint}_r \\
a_1
\end{bmatrix} \right) \cdot u_{\text{row}},
\]

where right-multiplication by \( u_{\text{row}} \) extracts the \( i_{\text{row}} \)-th column of the matrix.

• \( E_2 \), the event that the recovery of the single element in the “first level of PIR” fails, i.e., that

\[
\text{Round}_\Delta (\hat{d}) / \Delta \neq \text{db} [i_{\text{row}}, i_{\text{col}}].
\]

We make use of the following two propositions:

**Proposition E.2: Under the parameters in Theorem E.1,**

\[
\Pr[E_1] \leq \frac{\kappa(n + 1)}{(k(n + 1) + 1)} \cdot \delta.
\]

**Proof.** DoublePIR’s recovery routine computes:

\[
\begin{bmatrix}
\hat{h}_i \\
a_1
\end{bmatrix} \leftarrow \text{Recomp} \left( \text{Round}_\delta \left( \begin{bmatrix}
\hat{h}_i \\
a_1
\end{bmatrix} \right) / \Delta \right) \in \mathbb{Z}_{q}^{n + 1}.
\]

Define \( \text{db}_2 = \left[ \begin{bmatrix}
\text{hint}_r \\
a_1
\end{bmatrix} \in \mathbb{Z}_q^{\kappa(n + 1) \times \ell} \right \rangle \) and let \( E \) be the event that

\[
\text{Round}_\Delta \left( \begin{bmatrix}
\hat{h}_i \\
a_1
\end{bmatrix} \right) / \Delta \neq \text{db}_2 \cdot u_{\text{row}}.
\]

We have that \( \Pr[E] \geq \Pr[E_1] \) as \( E_1 \subset E \). By rewriting terms:

\[
\begin{bmatrix}
\hat{h}_i \\
a_1
\end{bmatrix} = \begin{bmatrix}
\text{ans}_h - \text{hint}_c \cdot s_2 \\
\text{ans}_s - \hat{h} \cdot s_2
\end{bmatrix}
\]

\[
= \begin{bmatrix}
\text{hint}_r \cdot e_2 - (\text{hint}_r \cdot A_2) \cdot s_2 \\
\text{ans}_s - e_2 - (\text{ans}_s \cdot A_2) \cdot s_2
\end{bmatrix}
\]

\[
= \begin{bmatrix}
\text{hint}_r \cdot (A_2 \cdot s_2 + e_2 + \Delta \cdot u_{\text{row}}) - \text{hint}_r \cdot A_2 \cdot s_2 \\
\text{ans}_s \cdot (A_2 \cdot s_2 + e_2 + \Delta \cdot u_{\text{row}}) - \text{ans}_s \cdot A_2 \cdot s_2
\end{bmatrix}
\]

\[
= \text{db}_2 \cdot e_2 + \Delta \cdot \text{db}_2 \cdot u_{\text{row}}.
\]

Comparing this with Equation (4), we see that \( E \) happens if and only if \( \|\text{db}_2 \cdot e_2\|_2 \geq \Delta / 2 \). The vector \( e := \text{db}_2 \cdot e_2 \) consists of \( \kappa \cdot (n + 1) \) elements, which we denote as \( e_1, \ldots, e_{\kappa \cdot (n + 1)} \).

As in our correctness proof for SimplePIR, we use a concentration inequality [68, Lemma 2.2][12, Lemma 2.4] on each of these terms: since \( \chi \) is the discrete Gaussian distribution with variance \( \sigma^2 = \frac{\chi^2}{2\pi} \) for some \( s > 0 \), for every \( j \in \kappa \cdot (n + 1) \) and any \( T > 0 \), it holds that,

\[
\Pr \left[ |e_j| \geq T \cdot \|\text{db}_2 [j, \cdot]\|_2 \right] < 2 \exp(-\pi \cdot T^2),
\]

where \( \|\cdot\|_2 \) is the Euclidean norm. Note that since we can represent the elements in \( \text{db}_2 \) in the range \((-p/2, p/2] \), we have that \( \|\text{db}_2 [j, \cdot]\|_2 \leq \sqrt{T} \cdot (p/2) = \sqrt{T} \cdot p/2 \). Therefore, for every \( j \in \kappa \cdot (n + 1) \), for any \( T > 0 \), it holds that,

\[
\Pr \left[ |e_j| \geq T \cdot s \cdot \sqrt{T} \cdot p/2 \right] < 2 \exp(-\pi \cdot T^2).
\]

Now, we take \( T = \Delta / (2s \cdot \sqrt{T} \cdot p/2) \), and we see that, for every \( j \in \kappa \cdot (n + 1) \),

\[
\Pr \left[ |e_j| \geq \Delta / 2 \right] < \frac{\delta}{\kappa(n + 1) + 1},
\]

as long as

\[
2 \exp \left( -\pi \cdot \left( \frac{\Delta}{2s \cdot \sqrt{T} \cdot p/2} \right)^2 \right) \leq \frac{\delta}{\kappa(n + 1) + 1}.
\]

Substituting \( \Delta = |q/p| \) and \( s = \sigma \cdot \sqrt{2\pi} \), we rewrite the second equation as:

\[
|q/p| \geq \sigma \cdot p \cdot \sqrt{2\ell \cdot \ln \left( \frac{2\kappa(n + 1) + 1}{\delta} \right)}.
\]

By Equation (3), this condition holds. Thus, we have shown that, for each \( j \in \kappa \cdot (n + 1) \), \( |e_j| < \Delta / 2 \) holds except with probability \( \frac{\delta}{\kappa(n + 1) + 1} \). Therefore, by a union bound, all \( e_1, \ldots, e_{\kappa \cdot (n + 1)} \) have an absolute value smaller than \( \Delta / 2 \) with probability \( \frac{\kappa(n + 1)}{\kappa(n + 1) + 1} \cdot \delta \), which completes the proof.

**Proposition E.3: Under the parameters in Theorem E.1,**

\[
\Pr[E_2 | \neg E_1] \leq \frac{1}{\kappa(n + 1) + 1} \cdot \delta.
\]

**Proof.** If \( \neg E_1 \) occurs, we know that

\[
\begin{bmatrix}
\hat{h}_i \\
a_1
\end{bmatrix} = \text{Recomp} \left( \begin{bmatrix}
\text{hint}_r \\
a_1
\end{bmatrix} \right) \cdot u_{\text{row}}
\]

\[
= \begin{bmatrix}
A_i^T \cdot \text{db}^T \\
e_1^T \cdot \text{db}^T
\end{bmatrix} \cdot u_{\text{row}}.
\]

Therefore,

\[
\hat{d} = a_1 - s_1 \cdot \hat{h}_1
\]

\[
= (e_1^T \cdot \text{db}^T - s_1 \cdot A_i^T \cdot \text{db}^T) \cdot u_{\text{row}}
\]

\[
= ((s_1^T \cdot A_i^T + e_1^T + \Delta u_{\text{col}}^T) \cdot \text{db}^T - s_1 \cdot A_i^T \cdot \text{db}^T) \cdot u_{\text{row}}
\]

\[
= e_1^T \cdot \text{db}^T \cdot u_{\text{row}} + \Delta u_{\text{col}}^T \cdot \text{db}^T \cdot u_{\text{row}}.
\]

Thus, we see that Recover outputs the correct database element, \( \text{db} [i_{\text{row}}, i_{\text{col}}] \), if and only if \( e_1^T \cdot \text{db}^T \cdot u_{\text{row}} \leq \Delta / 2 \). By essentially the same analysis as in Proposition E.2, the event
that $|e^T \cdot d b^T \cdot u_{row}| \geq \Delta/2$ happens occurs with probability at most $\frac{1}{\kappa(n+1) + 1} \cdot \delta$, given that the condition

$$|q/p| \geq \sigma \cdot p \cdot \sqrt{2m \cdot \ln \left(2\kappa(n+1) + 1\right)}$$

holds, which is true by Equation (3).

Combining the two propositions, we conclude that DoublePIR’s correctness error is upper bounded by

$$\Pr[E_1 \lor E_2] \leq \Pr[E_1] + \Pr[E_2 \lor \neg E_1] \leq \delta.$$  

security. DoublePIR’s security follows from the hardness of LWE with a reused LWE matrix [83]. We rely on the following lemma:

Lemma E.4. Let $N \in \mathbb{N}$ be the database size, $t, m \in \mathbb{N}$ be the database dimensions (such that $t \cdot m \geq N$), $(n, q, \chi)$ be the LWE parameters, and $A_1 \in \mathbb{Z}_q^{m \times n}$ and $A_2 \in \mathbb{Z}_q^{t \times n}$ be the random LWE matrices used in DoublePIR. For any $i \in [N]$, we define the distribution

$$Q_i = \{(A_1, A_2, qu_i) : \ldots, qu_i \leftarrow \text{Query}(i)\}.$$ 

If the $(n, q, \chi)$-LWE problem with max$(\ell, m)$ samples is $(T, \epsilon)$-hard, then any algorithm running in time $T - O(n \cdot \ell + m)$ has success probability at most $2\epsilon$ in distinguishing $Q_i$ from the distribution $D = \{(A_1, A_2, (r_1, r_2)) : r_1 \leftarrow \mathbb{Z}_q, r_2 \leftarrow \mathbb{Z}_q^{t \times n}\}$.

Proof. Consider any index $i \in [N]$, and decompose $i$ into the pair of coordinates $(i_{row}, i_{col}) \in [\ell] \times [m]$ as done in DoublePIR’s Query routine. Let $u_{row} \in \mathbb{Z}_q^m$ denote unit vector $i_{row}$ in $\mathbb{Z}_q^m$ and $u_{col}$ denote unit vector $i_{col}$ in $\mathbb{Z}_q^t$. We define the following distribution:

$$H_i = \{(A_1, A_2, (r_1, A_2s_2 + e_2)) : r_1 \leftarrow \mathbb{Z}_q^m, s_2 \leftarrow \mathbb{Z}_q, e_2 \leftarrow \mathbb{Z}_q^{t \times n}\}.$$ 

Now, consider any algorithm $A$ that runs in time $t$ and distinguishes between distributions $Q_i$ and $D$ with probability $p$. Let $p_0, p_1, p_2$ be the probabilities that $A$ outputs $1$ when given samples from $Q_i, H_i$, and $D$ respectively. Thus, by definition, it must hold that $|p_0 - p_2| = p$. From the triangle inequality we see that $|p_0 - p_1| + |p_1 - p_2| \geq p$.

Then, using $A$ as a subroutine, we build an algorithm $B_1$ that distinguishes between the $(n, q, \chi)$-LWE problem with $m$ samples and the uniform distribution, in time $t + O(m \cdot n + \ell)$ and with success probability $|p_0 - p_1|$ because the $(n, q, \chi)$-LWE problem with $m$ samples is $(T, \epsilon)$-hard, if $t \leq T - O(m \cdot n + \ell)$, it must hold that $|p_0 - p_1| \leq \epsilon$. Similarly, we build an algorithm $B_2$ that distinguishes between the $(n, q, \chi)$-LWE problem with $\ell$ samples and the uniform distribution in time $t + O(m \cdot \ell)$ and with success probability $|p_1 - p_2|$ because the $(n, q, \chi)$-LWE problem with $\ell$ samples is $(T, \epsilon)$-hard, if $t \leq T - O(m \ell + \ell)$, it must hold that $|p_1 - p_2| \leq \epsilon$.

Thus, if $t \leq T - O(m \cdot n + \ell)$, we see that $2\epsilon \geq |p_0 - p_1| + |p_1 - p_2| \geq p$. We have shown that any algorithm $A$ that runs in time $T - O(m \cdot n + \ell)$ can distinguish between $Q_i$ and $D$ with probability at most $2\epsilon$.

Algorithm 3 $B_1$, on input $A_1, b_1$:

- Compute $c_1 \leftarrow b_1 + [q/p] \cdot u_{row}$.
- Sample $s_2 \leftarrow \mathbb{Z}_q, e_2 \leftarrow \mathbb{Z}_q^{t \times n}$.
- Compute $c_2 \leftarrow (A_2s_2 + e_2) + [q/p] \cdot u_{row}$.
- Output $A(A_1, A_2, (c_1, c_2))$.

Algorithm 4 $B_2$, on input $A_2, b_2$:

- Sample $r_1 \leftarrow \mathbb{Z}_q^m$.
- Compute $c_2 \leftarrow b_2 + [q/p] \cdot u_{row}$.
- Output $A(A_1, A_2, (r_1, c_2))$.

Lemma E.4 states that any algorithm running in time $T - O(n \cdot \ell + m)$ can distinguish the queries made by a client in DoublePIR from random vectors with success probability at most $2\epsilon$. Therefore, any algorithm running in time $T - O(n \cdot \ell + m)$ can distinguish the queries made by a client in DoublePIR to any pair of indices $i \in [N]$ and $j \in [N]$ with success probability at most $4\epsilon$. Thus, we have shown that DoublePIR is $(T - O(n \cdot \ell + m), 4\epsilon)$-secure.

DoublePIR also meets the $Q$-query security definition that we give in Appendix C.2. A hybrid argument shows that:

Corollary E.5 ($Q$-query security of DoublePIR). For any sequence $I \in [N]^Q$ of $Q$ indices, we define $D_I$ to be the query distribution that it induces, i.e.,

$$D_I = \{(A_1, A_2, qu_k) : \ldots, qu_k \leftarrow \text{Query}(I_k)\}_{k \in [Q]}$$

If the $(n, q, \chi)$-LWE problem with max$(\ell, m)$ samples is $(T, \epsilon)$-hard, then $D_I$ is $(T - O(Q \cdot (n \cdot \ell + m)), 2QE)$-indistinguishable from the random query distribution.

E.3 Additional extensions and optimizations

The SimplePIR optimizations involving fast matrix multiplication algorithms (that we outline in Appendix C.3) apply to DoublePIR as well. We list some further extensions and efficiency improvements to DoublePIR in this section.

Handling database updates. When the database contents change, the server in DoublePIR needs to update its preprocessed hints, hint$_I$ and hint$_c$ (see Remark 3.1). In more detail, when $c$ rows of the database matrix change (for some number $c \geq 0$), the server needs to:

- perform $O(c \cdot m \cdot n + c \cdot \kappa \cdot n)$ operations in $\mathbb{Z}_q$, and
- send $\min(c \cdot \kappa \cdot n, \kappa \cdot n^2)$ elements in $\mathbb{Z}_q$ back to the client.

This update procedure works as follows. In DoublePIR, the server computes the hints as $\text{hint}_I \leftarrow \text{Decomp}(A_1^T \cdot d b^T)$ and $\text{hint}_c \leftarrow [\text{hint}_c \cdot A_2$. For each row $d \in \mathbb{Z}_q^m$ of the database that has changed, the server can update the corresponding columns of $\text{hint}_c$ to be $u \leftarrow \text{Decomp}(A_1^T \cdot d^T) \in \mathbb{Z}_q^{n}$. To update hint$_c$,
for each row of the database that has changed, the server would then have to add the outer product between the column vector, $u$, and the corresponding row of $A_3$, to hint$_c$. The server can perform this computation and send the updated hint$_c$ back to the client; or, if fewer than $n$ rows of the database were changed, the server can send only the associated column vectors, $u$, back to the client (to save on bandwidth) and have the client update its hint$_c$ locally. Again, additions and deletions of rows from the database can be handled similarly.

Reducing the client storage, when the client makes a bounded number of queries. If the client knows ahead of time that it will only make $Q \ll n$ queries, it can reduce its local storage to $Q \cdot k \cdot n$ (rather than $k \cdot n^2$) elements in $\mathbb{Z}_q$. To do so, the client samples $Q$ pairs of LWE secrets $(s_1, s_2)$ in advance (e.g., using a pseudorandom function). Then, rather than store hint$_c$ in its entirety, the client precomputes and stores only the information that it will need for recovery: for each of the $Q$ queries it intends to make, the client precomputes hint$_{c} \cdot s_2 \in \mathbb{Z}_q^{n}$ (where $s_2$ denotes the the secret key used for the corresponding query). Finally, the client discards hint$_c$.

In theory, the client storage could be reduced even further by applying the local rounding trick (see Appendix C.3) to the precomputed information, hint$_c \cdot s_2$, stored by the client. After doing so, the client would store only a single element in $\mathbb{Z}_q$—namely, $s_2^T \cdot \text{Recom}_3(\text{hint}_c \cdot s_2)$—for each query it intends to make. However, doing so would require using a much larger value of $\lceil q/p \rceil$ to maintain correctness and is thus not profitable in our parameter regime.

\section*{F Additional material on our private set-membership data structure}

\subsection*{F.1 Syntax and properties}

We define the syntax and security properties for our approximate private set membership data structure. The data structure is parameterized by a universe $\mathcal{U} \subseteq \{0,1\}^*$ of possible strings and consists of two routines:

**Setup($S$) $\rightarrow$ $D$.** Take as input a set of strings $S \subseteq \mathcal{U}$ and output a data structure $D \in \{0,1\}^{a \times b}$, where $a, b \in \mathbb{N}$ can depend on $|S|$.

**Query($\sigma$) $\rightarrow$ $(i, j)$.** Given a candidate string $\sigma \in \mathcal{U}$, output an index $(i, j) \in [a] \times [b]$ in the data structure $D$ to probe. If $\sigma \in S$, it holds that $D_{i,j} = 1$.

**Properties.** For a set $S \subseteq \mathcal{U}$ and string $\sigma \in \mathcal{U}$, define

$$\text{Accept}(S, \sigma) := \Pr \left[ D_{i,j} = 1 : (i, j) \leftarrow \text{Query}(\sigma) \right]$$

where the probability is taken only over the randomness of the Query algorithm.

**Correctness.** An approximate membership test is correct if, for all $S \subseteq \mathcal{U}$ and $\sigma \in S$, $\text{Accept}(S, \sigma) = 1$.

**Constant adversarial false-positive rate.** An approximate membership test has adversarial false-positive rate $\epsilon$ if, for all $S \subseteq \mathcal{U}$ and $\sigma \in S$, $\text{Accept}(S, \sigma) \leq \epsilon$.

**Oblivious reads.** An approximate membership test supports oblivious reads if the row of the data structure that the Query algorithm probes reveals no information about the query string $\sigma$. In other words, for all strings $\sigma_0, \sigma_1 \in \mathcal{U}$, the following distributions of the row indices are identical:

$$\{i : (i, \_ \leftarrow \text{Query}(\sigma_0)) \} \approx \{i : (i, \_ \leftarrow \text{Query}(\sigma_1)) \}.$$

In a deployment, to probe the element at row $i$ and column $j$ in the data structure, the client sends $i$ in the clear, along with a PIR query for $j$, to the server. The server executes the PIR scheme over the $i$-th row, and sends the PIR answer (and, if needed, the client hint for that row) back to the client. As the reads are oblivious, the server learns nothing about $\sigma$. Performing PIR over only a row of the data structure (rather than the whole data structure) will be the source of our $A$-fold performance improvements compared to related approaches.

\subsection*{F.2 Our approximate membership test}

Our construction is parameterized by integers $a, k \in \mathbb{N}$ and a set size $N$. Our data structure then maps the set of strings $S$ into a matrix of $a$-by-$(kN)$ bits. The construction uses cryptographic hash functions $H_1, \ldots, H_a : [k] \rightarrow [kN]$, which we model as independent random oracles [14] and which are chosen after the set $S$ has been fixed.

**Setup($S$) $\rightarrow$ $D \in \{0,1\}^{a \times kN}$.**
- Let $D \in \{0,1\}^{a \times kN}$ be the all-zeros matrix.
- For each $i \in [a]$ and $\sigma \in S$, set $D_{i,H_i(\sigma)} = 1$.
- Return $D$.

**Query($\sigma$) $\rightarrow$ $(i, j) \in [a] \times [kN]$.**
- Choose $i \leftarrow [a]$, and output $(i, H_i(\sigma))$.

\subsection*{F.3 Security analysis}

**Proposition F.1:** The approximate membership-test data structure (**Setup, Query**), on parameters $a \geq 2 \log(|\mathcal{U}| + \lambda)$ and $k \geq 8$, is correct, has false-positive rate $1/2$, and has oblivious reads. The construction fails with probability $2^{-\lambda}$, over the choice of the hash functions modeled as independent random oracles. Concretely, on $|\mathcal{U}| = 2^{56}$, taking $k = 8$ and $a = 768$ gives false-positive rate $1/2$ and failure probability $2^{-128}$.

**Proof.** Correctness and oblivious reads follow by construction. Constant adversarial false-positive rate is proved in Lemma F.2, which follows. \hfill \square

**Lemma F.2.** The approximate membership-test data structure (**Setup, Query**), on parameters $a$ and $k$ has adversarial false-positive rate at most $c$ and fails with probability $2^{-\lambda}$, for any $c \in (0,1)$ that satisfies $|\mathcal{U}| \left(\frac{a}{k}\right) k^{-ca} \leq 2^{-\lambda}$.
When \( k \geq 8 \) and taking \( c = 1/2 \), we get a data structure with adversarial false-positive rate \( 1/2 \) and failure probability at most \( 2^{-\lambda} \), as long as \( |\mathcal{U}| 2^{-\lambda/2} \leq 2^{-\lambda} \).

**Proof.** Fix any set \( S \subseteq \mathcal{U} \) and consider \( D \leftarrow \text{Setup}(S) \). Consider any \( e \in (0, 1) \) that satisfies \( |\mathcal{U}| (\frac{e^a}{c^a}) k^{-ca} \leq 2^{-\lambda} \).

For string \( \sigma \in \mathcal{U} \setminus S \), let \( \text{Bad}_\sigma \) be the event, over the random choice of the random oracle, that there is a set of rows \( R \subseteq [a] \) of size \( ca \), such that for all \( i \in R \), \( D_i H_i(\sigma) = 1 \). First, we bound the probability, over the choice of the random oracle, that there exists any bad string \( \sigma \).

In particular, fix a string \( \sigma \in \mathcal{U} \setminus S \). Now we analyze the event \( \text{Bad}_\sigma \) as follows. Each row of \( D \) contains at most \( |S| = N \) ones and has \( kN \) entries total. Thus, an independently sampled random element in \( D \) is non-zero with probability at most \( k^{-1} \). For a particular set \( R \subseteq [a] \) of size \( ca \), let \( \text{Bad}_{\sigma, R} \) be the event that for all \( i \in R \), \( D_i H_i(\sigma) = 1 \). Since the hash functions are modelled as random oracles, we have that \( \Pr[\text{Bad}_{\sigma, R}] \leq k^{-ca} \).

By a union bound over all possible sets \( R \),

\[
\Pr[\text{Bad}_{\sigma}] = \Pr \left[ \bigvee_{R \subseteq [a]} \text{Bad}_{\sigma, R} \right] \leq |\mathcal{U}| \cdot \Pr[\text{Bad}_{\sigma}] \leq |\mathcal{U}| \cdot \left( \frac{a}{ca} \right) \cdot k^{-ca}.
\]

Let \( \text{Bad} := \bigvee_{\sigma \in \mathcal{U} \setminus S} \text{Bad}_\sigma \). By a union bound over all possible strings \( \sigma \), we get that:

\[
\Pr[\text{Bad}] \leq |\mathcal{U}| \cdot \Pr[\text{Bad}_\sigma] \leq |\mathcal{U}| \cdot \left( \frac{a}{ca} \right) \cdot k^{-ca}.
\]

So, with probability \( 1 - |\mathcal{U}| \left( \frac{a}{ca} \right) k^{-ca} \) over the choice of the random oracles, there do not exist any bad strings \( \sigma \).

Now, consider the event \( \neg \text{Bad} \) (i.e., there exists no bad string). In this case, for any \( \sigma \in \mathcal{U} \setminus S \), we know that, with probability at most \( c \) (over the random coins of Query), the query algorithm will sample a row \( i \) such that \( D_i H_i(\sigma) = 1 \). Thus, we know that:

\[
\text{Accept}(S, \sigma) = \Pr_i [D_i H_i(\sigma) = 1] \leq c,
\]

where the probability is taken over the random choice of \( i \) by the Query algorithm.

Finally, taking \( k \geq 8 \) and \( c = 1/2 \), we see that \( \left( \frac{a}{2a/2} \right) \leq 2^a \) and \( k^{-ca} \leq 2^{-3a/2} \), which completes the proof. \( \square \)

### G Additional implementation material

In Figure 15, we give a code listing for the core of SimplePIR (without the extensions of Section 4.3). We do not include the code for the following helper functions:

- **MatrixRand**, which takes as input a matrix height, a matrix width, and the modulus to be used for the matrix entries, and returns a uniformly random matrix of the given dimensions.
- **MatrixGaussian**, which takes as input a matrix height, a matrix width, and the modulus to be used for the matrix entries.

```go
// Data types
type Matrix struct {
    rows uint
    cols uint
    data []uint
}

type Params struct {
    n uint // LWE secret dimension
    db_height uint // DB height
    db_width uint // DB width
    q uint // ciphertext modulus
    p uint // plaintext modulus
}

// SimplePIR methods
func Init(p Params) Matrix {
    A := MatrixRand(p.db_height, p.n, p.q)
    return A // 'A' is a public parameter
}

func Setup(DB Matrix, A Matrix) Matrix {
    H := MatrixMul(DB, A)
    return H // 'H' is the client hint
}

func Query(i uint, A Matrix, p Params) (Matrix, Matrix) {
    s := MatrixRand(p.n, 1, p.q)
    err := MatrixGaussian(p.db_width, 1, p.q)
    query := MatrixMul(A, s)
    query.MatrixAdd(err)
    query[i % p.db_width] += (p.q / p.p)
    return s, query // 's' is the client state
}

func Answer(DB Matrix, query Matrix) Matrix {
    ans := MatrixMul(DB, query)
    return ans // 'ans' is the server's answer
}

func Recover(i uint64, H, ans, s Matrix, p Params) uint64 {
    interim := MatrixMul(H, s)
    ans.MatrixSub(interim)
    noised := ans.data[1 / p.db_width]
    denoised := Round(noised, (p.q / p.p))
    return denoised // the recovered database value
}
```

Figure 15: SimplePIR Go code.
entries, and returns a matrix of the given dimensions whose entries were sampled from the discrete gaussian distribution (with the appropriate, hard-coded standard deviation).

- MatrixMul, which takes as input two matrices and returns their product, over the appropriate field.
- MatrixAdd, which takes as input two matrices and returns their sum, over the appropriate field.
- MatrixSub, which takes as input two matrices and returns their difference, over the appropriate field.
- Round, which takes as input a value and a base and returns the value rounded to the nearest multiple of the base, and then divided by the base.

## H Additional evaluation material

### Figure 17: Server offline processing time, both initially and when a contiguous 1\% of the database changes, on databases of increasing size with 1-bit entries.

In this section, we evaluate the server preprocessing time, the client time, and the non-amortized communication of our new PIR schemes.

**Server and client time.** Figure 17 displays the server time to run the Setup algorithm, both when the entire database contents change (as done at least once, at the very beginning of a deployment) and when a small, contiguous fraction of the database contents are updated. On a 1 GB database, the server in SimplePIR and DoublePIR takes roughly 5 core-minutes to run Setup over the entire database. Figure 18 gives the client time to run the Query and Recover algorithms. On a 1 GB database, the client in DoublePIR takes roughly 0.1 core-seconds both to generate its query and to recover the value it queried; in SimplePIR, these costs are lower. Both the server time and the client time are measured using a single thread of execution (and are fully parallelizeable).

**Non-amortized communication.** Figure 20 displays the offline and online communication incurred by each PIR scheme, on a 1 GB database with entries of increasing length. On databases with short entries, DoublePIR requires tens of megabytes of offline communication, along with hundreds of kilobytes of online communication. As soon as the entry size exceeds roughly 100 bits, SimplePIR incurs less communication than DoublePIR: hundreds of megabytes in the offline phase and hundreds of kilobytes in the online phase. The schemes from related work that achieve the highest throughput (SpiralStream and SpiralStreamPack) require tens of megabytes of online communication, regardless of the entry size.

Finally, we give the throughput data displayed in Figure 9 in Table 19, along with the communication data displayed in Figures 6 and 7 in Table 16.

## I Artifact appendix

### I.1 Abstract

Our source code for our two new, high-throughput PIR schemes, SimplePIR and DoublePIR, is available under the MIT open-source license at https://github.com/ahenzinger/simplepir. SimplePIR and DoublePIR, including their extensions to support databases with long records and batch queries (cf. Sections 4.3 and 5.2), are implemented in roughly 1,400 lines of Go code, along with 200 lines of C (for the performance-critical matrix-multiplication routines). For each PIR scheme, the code implements the Setup, Query, Answer, and Recover routines. Our repository additionally contains a suite of correctness tests and performance benchmarks. To
<table>
<thead>
<tr>
<th>Entry size</th>
<th>1 bit</th>
<th>2 bits</th>
<th>4 bits</th>
<th>1 B</th>
<th>2 B</th>
<th>4 B</th>
<th>8 B</th>
<th>16 B</th>
<th>32 B</th>
<th>64 B</th>
<th>128 B</th>
<th>256 B</th>
<th>512 B</th>
<th>1 KB</th>
<th>2 KB</th>
<th>4 KB</th>
</tr>
</thead>
<tbody>
<tr>
<td>SealPIR</td>
<td>0.31</td>
<td>0.31</td>
<td>0.31</td>
<td>0.31</td>
<td>0.31</td>
<td>0.31</td>
<td>0.31</td>
<td>0.31</td>
<td>0.31</td>
<td>0.31</td>
<td>0.31</td>
<td>0.49</td>
<td>0.67</td>
<td>1.2</td>
<td>2.1</td>
<td></td>
</tr>
<tr>
<td>FastPIR</td>
<td>3.3 · 10^3</td>
<td>1.6 · 10^4</td>
<td>8.2 · 10^3</td>
<td>4.1 · 10^3</td>
<td>2.1 · 10^3</td>
<td>1.0 · 10^3</td>
<td>5.10</td>
<td>260</td>
<td>130</td>
<td>64</td>
<td>32</td>
<td>16</td>
<td>8.1</td>
<td>4.1</td>
<td>2.1</td>
<td>1.3</td>
</tr>
<tr>
<td>OnionPIR</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.42</td>
<td>0.55</td>
</tr>
<tr>
<td>Spiral</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.18</td>
<td>0.23</td>
</tr>
<tr>
<td>SpiralPack</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.22</td>
<td>0.21</td>
</tr>
<tr>
<td>SpiralStream</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>14</td>
<td>7.4</td>
</tr>
<tr>
<td>SimplePIR</td>
<td>1.4</td>
<td>1.5</td>
<td>1.5</td>
<td>1.5</td>
<td>1.5</td>
<td>1.5</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
</tr>
<tr>
<td>DoublePIR</td>
<td>0.5</td>
<td>0.5</td>
<td>0.5</td>
<td>0.66</td>
<td>1</td>
<td>1.8</td>
<td>3.1</td>
<td>5.8</td>
<td>11</td>
<td>22</td>
<td>43</td>
<td>86</td>
<td>170</td>
<td>340</td>
<td>690</td>
<td></td>
</tr>
</tbody>
</table>

Table 16: Per-query communication in MB, amortized over 100 client queries, on a 1 GB database with entries of increasing size.

<table>
<thead>
<tr>
<th>Num. queries per batch</th>
<th>SimplePIR effective throughput (GB/s)</th>
<th>DoublePIR effective throughput (GB/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9.9</td>
<td>7.4</td>
</tr>
<tr>
<td>2</td>
<td>14.3</td>
<td>10.4</td>
</tr>
<tr>
<td>4</td>
<td>26.8</td>
<td>17.5</td>
</tr>
<tr>
<td>8</td>
<td>49.6</td>
<td>28.7</td>
</tr>
<tr>
<td>16</td>
<td>100.4</td>
<td>41.8</td>
</tr>
<tr>
<td>32</td>
<td>199.8</td>
<td>58.6</td>
</tr>
<tr>
<td>64</td>
<td>394.3</td>
<td>75.9</td>
</tr>
<tr>
<td>128</td>
<td>670.2</td>
<td>85.7</td>
</tr>
<tr>
<td>256</td>
<td>1567.0</td>
<td>91.7</td>
</tr>
<tr>
<td>512</td>
<td>2832.6</td>
<td>98.9</td>
</tr>
<tr>
<td>1024</td>
<td>3611.2</td>
<td>103.2</td>
</tr>
</tbody>
</table>

Table 19: Effective PIR throughput, with an increasing batch size and a fixed-size hint, on a database consisting of 2^{33} \times 1-bit entries.

obtain our performance numbers, we run our benchmarks on an AWS EC2 c5n.metal instance.

### I.2 Description & Requirements

#### I.2.1 Security, privacy, and ethical concerns

None.

#### I.2.2 How to access

The source code for SimplePIR and DoublePIR is available at https://github.com/ahenzinger/simplepir/tree/438b4590aceedf76c7588b03125dfc0db39e361f.

#### I.2.3 Hardware dependencies

We run our evaluation on an AWS EC2 c5n.metal instance running Ubuntu 22.04. However, it is possible to run the SimplePIR and DoublePIR code on any machine with an installation of Go and of a C compiler (see Section I.2.4), though this might require amending the command-line flags passed to the C compiler.

#### I.2.4 Software dependencies

Running SimplePIR and DoublePIR requires installations of Go and GCC. We additionally require Python, NumPy, and Matplotlib to generate our evaluation plots.

#### I.2.5 Benchmarks

None.

### I.3 Set-up

#### I.3.1 Installation

Instructions for installing the required dependencies are given in the Setup section of https://github.com/ahenzinger/simplepir/blob/main/README.md. Users should install Go (tested with version 1.19.1) and GCC (tested with version 11.2.0) to run SimplePIR and DoublePIR. Users should additionally install Python (tested with Python3), NumPy, and Matplotlib to generate our evaluation plots.

#### I.3.2 Basic Test

To run all SimplePIR and DoublePIR correctness tests, users should run the command

go test

in the simplepir/pir directory. The suite of correctness tests runs SimplePIR and DoublePIR on random databases of fixed dimensions and checks that the PIR outputs are correct. The test suite should take roughly 2.5 minutes to run.

This command should produce logging output, followed by this message to indicate that all tests have passed:

PASS

ok  github.com/ahenzinger/simplepir/pir

### I.4 Evaluation workflow

#### I.4.1 Major Claims

Our paper makes the following claims:
SimplePIR performance. On a database 1 GB in size containing $2^{33}$ 1-bit entries, SimplePIR has:
1. a throughput of roughly 10 GB/s/core when running on an AWS EC2 c5n.metal instance,
2. 121 MB of offline download, and
3. 242 KB of online communication.
This is shown by experiment (E1), whose results are displayed in Table 8 in the body of our paper.

DoublePIR performance. On a database 1 GB in size containing $2^{33}$ 1-bit entries, DoublePIR has:
1. a throughput of roughly 7.4 GB/s/core when running on an AWS EC2 c5n.metal instance,
2. 16 MB of offline download, and
3. 345 KB of online communication.
This is shown by experiment (E2), whose results are displayed in Table 8 in the body of our paper.

Throughput with batching. SimplePIR and DoublePIR’s throughput increases when the client makes batches of many queries at once. This is shown by experiment (E3), whose results are displayed in Figure 9 in the body of our paper.

Application evaluation. On a database 8 GB in size containing $2^{36}$ 1-bit entries, DoublePIR has:
1. a throughput of roughly 7 GB/s/core when running on an AWS EC2 c5n.metal instance,
2. 16 MB of offline download, and
3. 756 KB of online communication.
This is shown by experiment (E4), whose results are reported in Section 8.2 in the body of our paper.

1.4.2 Experiments

SimplePIR performance [5 compute-minutes]: This experiment benchmarks (1) the communication and (2) the throughput of SimplePIR, when running on a 1 GB database consisting of $2^{33}$ 1-bit entries.

Run the command
```
LOG_N=33 D=1 go test -bench SimplePirSingle -timeout 0 -run=^$
```

from the simplepir/pir directory. The command will run SimplePIR 5 times on a database consisting of $2^{33}$ 1-bit entries, and print logging information including the communication and the per-core throughput of each run. The logging results are interpreted the same way as in (E1).

DoublePIR performance [5 compute-minutes]: This experiment benchmarks (1) the communication and (2) the throughput of DoublePIR, when running on a 1 GB database consisting of $2^{33}$ 1-bit entries.

Run the command
```
LOG_N=33 D=1 go test -bench DoublePirSingle -timeout 0 -run=^$
```

from the simplepir/pir directory. The command will run DoublePIR 5 times on a database consisting of $2^{33}$ 1-bit entries, and print logging information including the communication and the per-core throughput of each run. The logging results are interpreted the same way as in (E1).

Throughput with batching [1.5h compute-hours]: This experiment benchmarks SimplePIR’s and DoublePIR’s effective, per-core throughput, when run on batches of queries of increasing size, on a 1 GB database consisting of $2^{33}$ 1-bit entries.

Run the command
```
go test -bench PirBatchLarge -timeout 0 -run=^$
```

from the simplepir/pir directory. The command will run both SimplePIR and DoublePIR 5 times on a database consisting of $2^{33}$ 1-bit entries, with batch sizes ranging from 1 to 1024, and print logging information including the communication and the per-core throughput of each run. The logging results are interpreted the same way as in (E1).

This command produces the output files simple-batch.log and double-batch.log in the simplepir/pir directory. From the simplepir/eval directory, run the command
```
python3 plot.py -p batch_tput -f ../pir/simple-batch.log ../pir/double-batch.log -n SimplePIR DoublePIR
```

This command plots SimplePIR and DoublePIR’s effective, per-core throughput for various batch sizes, and writes this plot to the file throughput_with_batching.pdf. This command was used to generate Figure 9.

Application evaluation [40 compute-minutes]: This experiment benchmarks (1) the communication and (2) the per-core throughput of DoublePIR, when running on an 8 GB database consisting of $2^{36}$ 1-bit entries.

Run the command
```
LOG_N=36 D=1 go test -bench DoublePirSingle -timeout 0 -run=^$
```

for each run of SimplePIR, this experiment prints logging information that look as follows:

- Rate: 10177.282855 MB/s, indicating that SimplePIR’s throughput was 10,177 MB/s/core.
- Online download: 120,000,000 KB, indicating that SimplePIR’s offline download consists of 120 KB.

For each run of SimplePIR, this experiment prints logging information that look as follows:

- Offline download: 123572 KB, indicating that SimplePIR’s offline download consists of roughly 121 MB.
- Online upload: 120,000,000 KB, indicating that SimplePIR’s offline upload consists of 120 KB.
from the simplepir/pir directory. The command will run DoublePIR 5 times on a database consisting of $2^{36}$ 1-bit entries, and print logging information including the communication and the per-core throughput of each run. The logging results are interpreted the same way as in (E1).

1.5 Version

Based on the LaTeX template for Artifact Evaluation V20220926. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2023/.