Cryptography meets algorithms (15893) Lecture Notes

Lecture 3: Lower Bounds for PIR

Scribe: Diana Vieira Fernandes

February 8, 2024

In recent lectures, we showed how to construct a 2-server Private Information Retrieval (PIR) schemes with sublinear bandwidth, without relying on any cryptographic assumptions. One question is whether we can achieve sublinear bandwidth in the single-server setting. We know that using cryptography (e.g. fully homomorphic encryption), we can easily get a single-server PIR scheme with constant bandwidth. However, is it possible to get sublinear bandwidth without cryptographic assumptions? In today's lecture, we will prove that

1. *A perfect (or even statistical) PIR scheme without cryptographic assumptions requires linear bandwidth;*
2. We will prove an even stronger version of the lower bound, that is, *a single-server PIR scheme with non-trivial bandwidth implies Oblivious Transfer (OT).*

Even though the second lower bound implies the first one, we will still begin by proving the first one since its proof is simpler. The second lower bound shows interesting complexity theorectic implications of PIR: informally speaking, we need "public-key operations" to construct single-server PIR with non-trivial bandwidth, since OT is believed to be strictly stronger than one-way functions (which gives symmetric-key cryptography) [IR89].

The high-level idea of the first lower bound is to show that there exists an extractor, such that given any database DB and any query q, the extractor can extract the whole database given the communication script. This shows that the communication script has at least n-bit of entropy for a randomly sampled n-bit database, and thus it is at least n-bit long.

The idea of the second lower bound is construct an OT scheme from a PIR scheme with non-trivial bandwidth. The challenge in the proof arises from the fact that PIR has only one-sided privacy, but OT has two-sided privacy (as explained more later).

1 Information-Theoretic 1-Server PIR Requires Linear Bandwidth

The following theorem has been a folklore lower bound and is formalized by Damgård, Larsen and Nielsen [DLN19].

Theorem 1 ([DLN19])**.** *1-server PIR scheme with perfect correctness and perfect privacy must have $\Omega(n)$ bandwidth where $n = |\mathsf{DB}|$. Further, this lower bound holds regardless of the number of rounds or client/server computation.*

Notations. Given any database $\mathsf{DB} \in \{0,1\}^n$, any client query $i \in [n]$, we denote the PIR protocol's communication script as $\langle \mathsf{Server}(\mathsf{DB}, r_1) \leftrightarrow \mathsf{Client}(i, r_2) \rangle$ (if it's multi-round, we just concatenate all the exchanged messages). Here, r_1 and r_2 are the random coins consumed by the server and the client, respectively. By the definition of perfect correctness, there exists an algorithm $\mathsf{Reconstr}$, such that $\mathsf{Reconstr}\left(\langle \mathsf{Server}(\mathsf{DB}, r_1) \leftrightarrow \mathsf{Client}(i, r_2) \rangle, i, r_2\right) = \mathsf{DB}[i]$ with probability 1. That is, the $\mathsf{Reconstr}$ is the client-side algorithm to construct the final answer in the PIR protocol.

Proof. At a high level, the intuition of the proof is the folowing. By perfect privacy and perfect correctness of the PIR scheme, given any possible communication script C, a computationally unbounded extractor can extract all original database bits. Then, the communication script C can actually be seen as an encoding for the database, and the decoder just runs the extractor to reconstruct the database. This gives us a uniquely decodable scheme and by Shannon's source coding theorem, the expected length of the codeword has be at least n bits when the database is randomly sampled.

The following claim says that one can extract the entire database from the communication transcript of the PIR.

Claim 2. *Fix some $\mathsf{DB} \in \{0,1\}^n$. Fix an arbitrary $i \in [n]$, and arbitrary client and server coins r_1, r_2. Let $C = \langle \mathsf{Server}(\mathsf{DB}, r_1) \leftrightarrow \mathsf{Client}(i, r_2) \rangle$ be the transcript of the PIR protocol on DB, i, r_1, r_2. Then for any $j \in [n]$, there must exist some r_2' such that C is compatible with (j, r_2'). Further, $\mathsf{Reconstr}\left(C, j, r_2'\right) = \mathsf{DB}[j]$.*

In the above, the communication trascript C being compatible with (j, r_2') means that if we rerun the client's algorithm using input j, coins r_2', and the first $(r-1)$ messages it receives in C, it outputs the same r-th outgoing message as in C. Further, this holds for any r.

Proof of Claim 2. For fixed DB, r_1, transcript C happens with non-zero probability for query $i \in [n]$. By perfect privacy, transcript C must happen with non-zero probability for any query index $j \in [n]$. This means that there exists r_2' such that j, r_2' is compatible with C. This means that the transcript is also C when the PIR is executed on $\mathsf{DB}, r_1, j, r_2'$. By perfect correctness of the PIR scheme, it must be that $\mathsf{Reconstr}\left(C, j, r_2'\right) = \mathsf{DB}[j]$. □

Given Claim 2, we can construct the following encoding scheme. Notice that the encoder and the decoder algorithms need not be efficient.

- $\mathsf{Encode}(\mathsf{DB})$: Arbitrarily fix the client and server's random coins r_1 and r_2, and choose an arbitrary query $i \in [n]$, say $i = 1$. Given an n-bit database DB, the encoding for DB is the communication transcript $\langle \mathsf{Server}(\mathsf{DB}, r_1) \leftrightarrow \mathsf{Client}(i, r_2) \rangle$.
- $\mathsf{Decode}(C)$: Given a codeword C, the decoder algorithm will reconstruct the j-th bit of DB for any $j \in [n]$ as follows. The algorithm fixes j and enumerates r_2' until C is compatible with (j, r_2'). Then, the j-th bit of DB is reconstructed by $\mathsf{Reconstr}\left(C, j, r_2'\right)$.

Due to Claim 2, the above encoding scheme always correctly decodes. i.e., $\forall\ \mathsf{DB} \in \{0,1\}^n$, $\Pr[\mathsf{Decode}(\mathsf{Encode}(\mathsf{DB})] = 1$. Then, by Shannon's source coding theorem, we have the following where $H(\mathsf{DB})$ denotes the entropy of a randomly sampled DB:

$$\mathbf{E}_{\mathsf{DB} \xleftarrow{\$} \{0,1\}^n} \left[\mathsf{Encode}(\mathsf{DB})\right] \geq H(\mathsf{DB}) = n.$$

As a special case, if the communication length of the PIR scheme is fixed (i.e., does not depend on the server and client's inputs and coins), then it must be at least n bits long. □

Remark 1. [DLN19] extended the proof to statistical-correct and statistical-private PIR schemes.

2 Non-Trivial 1-Server PIR Implies Oblivious Transfer

Crescenzo, Malkin, and Ostrovsky [CMO00] showed that a single-server PIR with non-trivial bandwidth implies Oblivious Transfer (OT). 1-out-of-2 OT can be viewed as a special secure 2-party computation protocol for a "selection" functionality (as formally defined later). Kilian showed that OT is complete for realizing secure multi-party computation for any functionality, even in the presence of dishonest majority. OT is known to imply one-way functions (OWF). OT also implies key exchange, and the famous result of Impagliazzo and Rudich showed that one cannot construct OT from OWF with a blackbox reduction [IR89]. This gives some evidence that OT is likely strictly stronger than OWF. As mentioned, another way to interpret the result is that to get 1-server PIR with non-trivial bandwidth, we need "public-key operations".

In our lecture, we will show that 1-server PIR with non-trivial bandwidth implies *honest-receiver* OT. We note that Crescenzo, Malkin, and Ostrovsky [CMO00] also showed that how to construct *malicious-receiver* OT from 1-server PIR (with non-trivial bandwidth).

2.1 Definition of OT

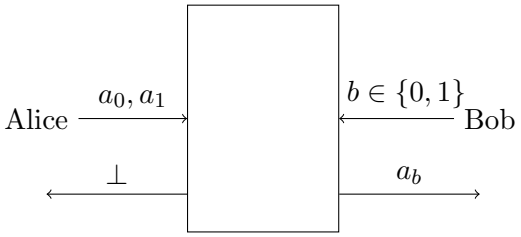

Figure 1: OT Functionality

Syntax. A 1-out-of-2 OT between Alice and Bob has the following abstraction:

- Alice has two bits a_0 and a_1, Bob has a single bit b. Bob wishes to learn a_b.
- Alice should not learn Bob's choice of b (Bob's privacy).
- Bob should not learn a_{1-b} (Alice's privacy).

Notations. The protocol's execution is denoted as

$$\begin{pmatrix} \mathsf{View}_A \\ \mathsf{View}_B \\ \mathrm{out}_B \end{pmatrix} = \langle \mathsf{Alice}(1^\lambda, a_0, a_1) \leftrightarrow \mathsf{Bob}(1^\lambda, b) \rangle,$$

where λ is the security parameter, and

- View_A is Alice's view, including Alice's random coins and the protocol transcript;
- View_B is Bob's view, including Bob's random coins and the protocol transcript;
- out_B is Bob's output.

Definition 3 (Correctness of OT)**.** Given any $a_0, a_1, b \in \{0,1\}^3$,

$$\Pr[(\cdot, \cdot, \mathsf{out}_B) \leftarrow \langle \mathsf{Alice}(1^\lambda, a_0, a_1) \leftrightarrow \mathsf{Bob}(1^\lambda, b) \rangle : \mathsf{out}_B = a_b \,] = 1 - \mathsf{negl}(\lambda).$$

That is, Bob should output the correct bit he tries to fetch with overwhelming probability.

We now see the privacy definitions. We focus on the case where Alice can be malicious and Bob is honest but curious, which means Alice may deviate from the protocol, but Bob follows the protocol honestly and only tries to break the privacy based on his local view.

Definition 4 (Sender's privacy against an honest-but-curious receiver)**.** For every probabilistic polynomial-time (PPT) reconstruction algorithm R, there exists a negligible function negl such that for all inputs $a_0, a_1, b \in \{0,1\}$, the following holds:

$$\Pr\left[\begin{array}{c}(a_0,a_1) \xleftarrow{\$} \{0,1\}^2 \\ (\cdot, \mathsf{View}_B, \cdot) \leftarrow \langle \mathsf{Alice}(1^\lambda, a_0, a_1) \leftrightarrow \mathsf{Bob}(1^\lambda, b)\rangle : \\ R(1^\lambda, \mathsf{View}_B) = a_{1-b}\end{array}\right] < \frac{1}{2} + \mathsf{negl}(\lambda)$$

Definition 5 (Receiver's privacy against a malicious sender)**.** For any PPT adversary A^* representing a malicious sender (Alice), for any PPT reconstruction algorithm R^*, there exists a negligible function negl that the following holds:

$$\Pr\left[\begin{array}{c}b \xleftarrow{\$} \{0,1\} \\ (\mathsf{View}_A, \cdot, \cdot) \leftarrow \langle A^*(1^\lambda, a_0, a_1) \leftrightarrow \mathsf{Bob}(1^\lambda, b)\rangle : \\ R^*(1^\lambda, \mathsf{View}_A) = b\end{array}\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

Remark 2. PIR can also be viewed as a special 2-party computation protocol with the following additional features: 1) we only need one-sided privacy, and 2) PIR has special efficiency requirements on the communication (otherwise a trivial way is to simply download the whole database).

To construct OT from PIR, the main challenge arises from the following discrepancy:

1. PIR has only *one-sided privacy*, that is, the server should not learn the client's query but there is no privacy guarantee for the server's database;
2. However, OT has *two-sided privacy*, that is, both Alice and Bob's privacy must be protected.

Therefore, the main challenge is how to prove sender privacy when the underlying PIR does not directly offer it. As you shall see in the proof, sender privacy will follow from the fact that the PIR scheme is bandwidth-efficient.

2.2 Proof

We now show that any 1-server PIR scheme for an n-bit database with at most $n/2$ bandwidth implies OT.

Constructing OT from PIR [CMO00]. The construction of honest-receiver OT from PIR is shown in Figure 2. Basically, Alice samples a random database, and Bob samples a random index, and the two run a PIR protocol. This is repeated m times — let $\mathsf{DB}_1, \ldots, \mathsf{DB}_m$ be the sampled databases and $i_1, \ldots, i_m$ be the indices queried by Bob. Next, Bob samples m independent random indices denoted $i'_1, \ldots, i'_m$. He sends both the real indices $i_1, \ldots, i_m$ and the random ones $i'_1, \ldots, i'_m$ to Alice, and the order in which he sends them depends on Bob's input b of the OT protocol. Alice uses the database values at these indices to XOR her inputs a_0 and a_1 respectively, and sends both answers back to Bob. Bob can only decode one of them and reconstruct a_b, since it only knows the database values at the real indices $i_1, \ldots, i_m$.

Phase 1. Repeat the following process m times (indexed by j):

- Alice samples $\mathsf{DB}_j \xleftarrow{\$} \{0,1\}^n$
- Bob samples $i_j \xleftarrow{\$} [n]$
- Alice and Bob execute the PIR protocol acting as the server and the client, respectively. Let x_j be Bob's output.

Phase 2.

- Bob samples $i'_1, \ldots, i'_m \xleftarrow{\$} [n]^m$
- Bob sends the following tuples to Alice:

$$\begin{cases} (i_1, \ldots, i_m), (i'_1, \ldots, i'_m), & \text{if } b = 0 \\ (i'_1, \ldots, i'_m)(i_1, \ldots, i_m), & \text{if } b = 1 \end{cases}$$

- Alice parses the message as $(t^0_1, \ldots, t^0_m), (t^1_1, \ldots, t^1_m)$.
- Alice returns the following two bits to Bob:

$$c_0 \leftarrow a_0 \oplus \mathsf{DB}_1[t^0_1] \oplus \cdots \oplus \mathsf{DB}_m[t^0_m]$$

$$c_1 \leftarrow a_1 \oplus \mathsf{DB}_1[t^1_1] \oplus \cdots \oplus \mathsf{DB}_m[t^1_m]$$

- Bob can reconstruct a_b from c_b because it knows $x_1 = \mathsf{DB}[i^b_1], \ldots, x_m = \mathsf{DB}[i^b_m]$.

Figure 2: Constructing an honest-receiver OT from PIR.

Correctness of the resulting OT follows directly from PIR's correctness. It is not hard to show Bob's privacy given the privacy of the underlying PIR. The most intersting part of the proof is showing Alice's privacy (i.e., sender privacy). To show this, we will make use of the fact that the PIR's communication transcript is short, and thus it cannot encode too much information about the entire database. This means that for a randomly sampled index, (even an unbounded) Bob does know too much information about the database at that index. This is also the place where we need to use the fact Bob is honest but curious, since we are trusting Bob to choose the indices $i'_1, \ldots, i'_m$ at random.

The key is to show for any fixed PIR instance, (even an unbounded) Bob cannot correctly predict the database's value at a random index with significant probability. If we can show this, we can use the following XOR amplification lemma, which informally says that the XOR of m bits each with some uncertainty will amplify the uncertainty exponentially fast.

Lemma 6. *Suppose $X_1, \ldots, X_n$ are binary random variables such that for each i, $\Pr[X_i = 1] = \frac{1}{2} + \delta_i$ where $\delta_i \in (-\frac{1}{2}, \frac{1}{2})$. Then, we have that*

$$\Pr[X_1 \oplus ... \oplus X_n = 1] = \frac{1}{2} + \prod_{i=1}^{n} (2\delta_i)$$

Proof. We can prove the statement using an inductive proof.

Base Case: The base case $\Pr[X_1 = 1] = \frac{1}{2} + \delta_1$ holds by definition.

Inductive Step: Suppose the statement holds for $\Pr[X_1 \oplus \ldots \oplus X_m = 1]$, we want to show that it holds for $\Pr[X_1 \oplus \ldots \oplus X_{m+1} = 1]$. Write $\Pr[X_1 \oplus \ldots \oplus X_i = 1] = \frac{1}{2} + p_m$. By a simple conditional probability calculation,

$$\Pr[X_1 \oplus \ldots \oplus X_{m+1} = 1] = \left(\frac{1}{2} + p_m\right) \cdot \left(\frac{1}{2} + \delta_{m+1}\right) + \left(\frac{1}{2} - p_m\right) \cdot \left(\frac{1}{2} - \delta_{m+1}\right)$$

Therefore, $\Pr[X_1 \oplus \ldots \oplus X_{m+1} = 1] = \frac{1}{2} + 2p_m\delta_{m+1}$ which gives the lemma.

□

For the rest of the proof, we only need to show that for each single copy, after executing the PIR, Bob can correctly guess the database at a random index with probability no more than $\frac{1}{2} + \delta$ for some constant δ, and the rest of the proof follows from the XOR lemma.

Given any $i \in [n]$, any reconstruction algorithm R, consider the following experiment.

$\underline{\mathsf{Expt}(1^\lambda, n, \mathsf{coin}_A, \mathsf{coin}_B, i, R)}$:

- $\mathsf{DB} \xleftarrow{\$} \{0,1\}^n$
- $(\cdot, \mathsf{View}_B) \leftarrow \langle \mathsf{PIR.Alice}(1^\lambda, \mathsf{DB}, \mathsf{coin}_A) \leftrightarrow \mathsf{PIR.Bob}(1^\lambda, i, \mathsf{coin}_B) \rangle$
- $r \xleftarrow{\$} [n]$;
- output 1 if $R(1^\lambda, \mathsf{View}_B, r, \mathsf{coin}_B) = \mathsf{DB}[r]$

Claim 7. *Fix $\lambda, n, \mathsf{coin}_A, \mathsf{coin}_B, i, R$ arbitrarily. Let $p = \Pr[\mathsf{Expt}(1^\lambda, n, \mathsf{coin}_A, \mathsf{coin}_B, i, R) = 1]$. Then,*

$$H(p) \geq \frac{n-l}{n},$$

where $H(p)$ is the binary entropy of p, n is the database size, and l is the communication script length in the PIR scheme.

Proof. Let Comm be the communication script in the PIR scheme. By definition of entropy, $H(\mathsf{Comm}) \leq l$. Denote $\mathsf{DB} = (y_1, \ldots, y_n)$. Let $z_j = R(1^\lambda, \mathsf{View}_B, j, \mathsf{coin}_B)$ for $j \in [n]$. Let $p_j = \Pr[y_j \neq z_j]$ and $p = \frac{1}{n}\sum_{j\in[n]} p_j$.
By Fano's inequality $^{(\triangle)}$:

$$H(p_j) \geq H(y_j|\mathsf{Comm})$$

By chain rule$^{(\star)}$:

$$H(\mathsf{DB}|\mathsf{Comm}) = \sum_{j=1}^{n} H(y_j|\mathsf{Comm}, y_{j-1}, \ldots, y_1) \leq \sum_{j=1}^{n} H(y_j|\mathsf{Comm}).$$

Thus,

$$H(\mathsf{DB}|\mathsf{Comm}) = H(\mathsf{DB}) - H(\mathsf{Comm}) + H(\mathsf{Comm}|\mathsf{DB}) \geq n - H(\mathsf{Comm}) \geq n - l,$$

Hence,

$$H(p) = H\left(\frac{1}{n}\sum_{j=1}^{n} p_j\right) \geq^{(\triangle)} \frac{1}{n}\sum_{j=1}^{n} H(p_j) \geq \frac{1}{n}\sum_{j=1}^{n} \frac{H(yg_j|\mathsf{Comm})}{n} \geq^{(\star)} \frac{n-l}{n}$$

Where $\triangle$ and $\star$ denote where each inequality is applied. □

The full proof can also be seen in [DLN19] and for the lemmas 4.5 (absolute difference in entropy between two probability distributions p and q on a finite set M is bounded above by the L_1-norm of their difference) and 4.6 (bounds the entropy of a function and is maximized by the uniform distribution) [DPP98].

Notes

Conditional Entropy

$$H(Y|X) = -\sum_{x \in D_X, y \in D_Y} p(x,y) \log_2 \frac{p(x,y)}{p(x)}$$

Entropy

Let X be a random variable taking values over a finite domain D_X.

$$H(X) = -\sum_{x \in D_X} p(x) \log_2 p(x)$$

Fact: $0 \leq H(X) \leq \log_2(|D_X|)$

Chain Rule

$$H(Y|X) = H(X) + H(Y|X)$$
$$H(X_1, \ldots, X_n) = \sum_{i=1}^{n} H(X_i|X_1, \ldots, X_{i-1})$$

Bayes Rule

$$H(Y|X) = H(X|Y) - H(X) + H(Y)$$

Binary Entropy Function

For $p \in [0,1]$:

$$H(p) = -p \log_2(p) - (1-p) \log_2(1-p)$$

Concavity

For $p, q \in [0,1]$ and $0 \leq \lambda \leq 1$:

$$H(\lambda p + (1-\lambda)q) \geq \lambda H(p) + (1-\lambda) H(q)$$

Fano's Inequality

Let X and Y be random variables with $X \in D_X$ and $Y \in D_Y$. Let $\hat{X} = f(Y)$ be a predictor of X based on the observations Y, and let $p = P(X \neq \hat{X})$.

$$H(X|Y) \leq H(p) + p \log_2(|D_X| - 1)$$

References

[CMO00] Giovanni Di Crescenzo, Tal Malkin, and Rafail M. Ostrovsky. Single database private information retrieval implies oblivious transfer. In *International Conference on the Theory and Application of Cryptographic Techniques*, 2000.

[DLN19] Ivan Damgård, Kasper Green Larsen, and Jesper Buus Nielsen. Communication lower bounds for statistically secure mpc, with or without preprocessing. Cryptology ePrint Archive, Paper 2019/220, 2019. `https://eprint.iacr.org/2019/220`.

[DPP98] I.B. Damgard, T.P. Pedersen, and B. Pfitzmann. Statistical secrecy and multibit commitments. *IEEE Transactions on Information Theory*, 44(3):1143–1151, 1998.

[IR89] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, STOC '89, page 44–61, New York, NY, USA, 1989. Association for Computing Machinery.