COL872: Quantum and Post-Quantum Cryptography

Problem Set 2

Due date: February 16th, 2023

Instructions

1. Assignments must be done in groups of size at most three. Each group must upload one submission, and mention the names of all group members.
2. You are welcome to discuss with other classmates and instructor, as well as refer to resources online. But if you do, please mention who all you collaborated with, or the online resources used.

This is version 2 of the assignment, uploaded on 09/02/23. Major edits: updated due date, fixed definition of witness indistinguishable proofs.

Questions

Question 1. Doubly Efficient Interactive Proofs *(10 points)*

This has been an active area of research since the work of Goldwasser, Kalai and Rothblum [GKR15].

In class, we saw an interactive protocol (the sumcheck protocol) for verifying very hard problems (e.g. counting the number of satisfying solutions to a 3SAT *formula). Interactive protocols can also be used for problems in* P*. The objective here is to verify solutions such that*

- *the verification time is much less than the time required to solve the problem (preferably linear in the input size).*
- *the prover's running time should not be much more than the time required to solve the problem.*

Since both the prover and verifier have nearly optimal running time, these protocols are called doubly efficient interactive protocols*.*

In this problem, we will develop a doubly efficient protocol for the disjoint sets problem. The problem is parameterized by two integers n, d, where $d = \log^2(n)$. The input is two sets of sets $\mathcal{S} = \{S_i\}_{i\in[n]}$ and $\mathcal{T} = \{T_i\}_{i\in[n]}$, where each $S_i, T_i \subseteq [d]$ (hence the input can be described in $O(n \cdot d) = \widetilde{O}(n)$ bits). The output is

Here $\widetilde{O}$ hides polylogarithmic factors.

$$\mathsf{DisjSet}(\mathcal{S},\mathcal{T}) = \left|\left\{(i,j) : S_i \cap T_j = \emptyset\right\}\right|$$

The problem can be solved in time $\widetilde{O}(n^2)$.

1. *Give a doubly-efficient protocol where the verifier runs in time $\widetilde{O}(n)$, and the prover runs in time $\widetilde{O}(n^2)$.*

   Hint: Express this computation as a polynomial in $O(\log n)$ variables, and then use the sumcheck protocol.

Question 2. Zero-knowledge protocols for group-theoretic problems *(20 points)*

Let $\mathbb{G}$ be a prime-order group of size $q = O(2^n)$. In Lecture 9, we will see a (honest-verifier) zero-knowledge proof-of-knowledge protocol for proving the knowledge of discrete log.

1. *(HVZK PoK for DDH - 5 points) Consider the following language.*

   $$\mathcal{L}_{\text{DDH}} = \left\{(g,h,u,v) \ : \ \exists\, a \in \mathbb{Z}_q \text{ s.t. } u = g^a, v = h^a\right\}$$

   Construct a honest-verifier zero-knowledge proof-of-knowledge protocol for $\mathcal{L}_{\text{DDH}}$. The protocol must have perfect completeness, the knowledge error must be $1/q$, and it should satisfy honest-verifier zero-knowledge property.

2. *(ZK protocol for $\overline{DDH}$ - 5 points) Next, consider the complement of $\mathcal{L}_{\text{DDH}}$, denoted by $\mathcal{L}_{\text{nDDH}}$ (defined below).*

   $$\mathcal{L}_{\text{nDDH}} = \left\{(g,h,u,v) \ : \ \forall\, a \in \mathbb{Z}_q, \text{ either } u \neq g^a \text{ or } v \neq h^a\right\}$$

   Construct a protocol for $\mathcal{L}_{\text{nDDH}}$. The protocol must have perfect completeness, constant soundness error and should satisfy zero-knowledge w.r.t auxiliary information.

3. *(HVZK PoK for k-out-of-t DDH - 10 points) Let k, t be two integers such that $k \leq t$. Consider the following language:*

   $$\mathcal{L}_{\text{DDH,k,t}} = \left\{ (g,h,u_1,v_1,\ldots,u_t,v_t) \ : \ \begin{array}{c} \exists \text{ indices } i_1,i_2,\ldots,i_k \in [t], \\ \exists \text{ exponents } a_1,a_2,\ldots,a_k \in \mathbb{Z}_q, \\ \text{s.t. } \forall\, j \leq k, u_{i_j} = g^{a_j} \text{ and } v_{i_j} = h^{a_j} \end{array} \right\}$$

   Construct a honest-verifier zero-knowledge proof-of-knowledge protocol for $\mathcal{L}_{\text{DDH,k,t}}$. The protocol must have perfect completeness, the knowledge error must be $1/q$, and it should satisfy honest-verifier zero-knowledge property.

   Hint: as a stepping stone, construct a protocol for 1-out-of-2 and 2-out-of-2 DDH satisfying the above properties.

Question 3. Impossibility of two-round zero-knowledge protocols with auxiliary information *(10 points)*

In class, we showed that truly non-interactive (unidirectional) protocols cannot satisfy the zero-knowledge property. In this problem, we will extend the above result, and prove that even two-round protocols are impossible for languages outside BPP.

This was first shown by Goldreich and Oren [GO94]. It was later extended by Barak, Lindell and Vadhan [BLV04] who showed that two-round protocols are impossible even if there is no auxiliary information.

1. *Prove that two-round protocols (where the verifier sends the first message and prover sends the second message) cannot satisfy the zero-knowledge property in the presence of auxiliary information. Describe the argument in full detail.*

   You can refer to [GO94], or discuss with me for hints.

Bonus Questions

Bonus Question 1. A different definition for zero-knowledge *(5 points)*

In class, we defined the zero knowledge property as follows: for every malicious verifier, there exists a simulator that can generate an indistinguishable view. The full formal definition is given below (we give the definition for computational zero knowledge, but we can also define perfect/statistical zero knowledge in a similar manner).

Definition (Zero knowledge w.r.t Auxiliary Information)**.** *Let* $(\mathbf{P}, \mathbf{V})$ *be an interactive proof system for language* $\mathsf{L} = (\mathsf{L}_{\text{yes}}, \mathsf{L}_{\text{no}})$*. We say that the proof system satisfies computational zero knowledge if for every (possibly malicious) p.p.t. verifier* $\mathbf{V}^*$ *and polynomial* p_1*, there exists a p.p.t. simulator* $\mathbf{S}$ *such that for every p.p.t. distinguisher* $\mathbf{D}^*$*, there exists a negligible function* μ *such that for every* $x \in \mathsf{L}_{\text{yes}}$*, every* $z \in \{0,1\}^{p_1(|x|)}$*,*

$$\Pr\left[\mathbf{D}^*\left(\mathsf{view}\langle \mathbf{P}, \mathbf{V}^*(z)\rangle(x)\right) = 1\right] - \Pr\left[\mathbf{D}^*\left(\mathbf{S}(x,z)\right) = 1\right] \leq \mu(|x|)$$

where the probabilities are taken over the randomness used by $\mathbf{P}, \mathbf{V}^*, \mathbf{S}$ *and* $\mathbf{D}^*$*.* ◊

Recall, we saw that one cannot have const. rd., public-coin, BB zero-knowledge protocols with negl. soundness error for NP-complete *languages. However, [Bar01] showed a const. rd., public-coin, (non-BB) zero-knowledge protocol with negl. soundness error for all* NP *languages.*

However, this definition is not completely satisfactory — it merely says that for every p.p.t. $\mathbf{V}^*$*, there* ***exists*** *a p.p.t. simulator such that it can simulate the adversary's view. This does not tell us how to find the simulator, given a description of the p.p.t. verifier. Note that the black-box zero-knowledge definition does not have this issue, since the simulator* $\mathbf{S}$ *is fixed first, and for every malicious verifier* $\mathbf{V}^*$*,* $\mathbf{S}^{\mathbf{V}^*}$ *simulates the verifier's view. Unfortunately, as we discussed in class, there exist protocols that satisfy zero-knowledge property, but do not satisfy black-box zero-knowledge.*

Consider the following definition which captures our intuition for the zero-knowledge property. Intuitively, it says that for every $\mathbf{V}^*$*, one can efficiently find the relevant simulator* $\mathbf{S}$ *using an efficient 'compiler'* Y *that maps* $\mathbf{V}^*$ *to* $\mathbf{S}$*.*

Definition (Compiler-based Zero knowledge w.r.t Auxiliary Information)**.** *Let* $(\mathbf{P}, \mathbf{V})$ *be an interactive proof system for language* $\mathsf{L} = (\mathsf{L}_{\text{yes}}, \mathsf{L}_{\text{no}})$*. We say that the proof system satisfies* ***compiler-based zero knowledge*** *if there exists an efficient deterministic compiler* Y *such that for every (possibly malicious) p.p.t. verifier* $\mathbf{V}^*$*,*

polynomial p_1 and distinguisher $\mathbf{D}^*$, there exists a negligible function μ such that for every $x \in \mathsf{L}_{\text{yes}}$, every $z \in \{0,1\}^{p_1(|x|)}$,

$$\Pr\left[\mathbf{D}^*\left(\text{view}\langle \mathbf{P}, \mathbf{V}^*(z)\rangle(x)\right) = 1\right] - \Pr\left[\mathbf{D}^*\left(\mathbf{S}(x,z)\right) = 1\right] \leq \mu(|x|)$$

where $\mathbf{S} = Y(\mathbf{V}^*)$, and the probability is over the randomness used by $\mathbf{P}, \mathbf{V}^*, \mathbf{S}$ and $\mathbf{D}^*$. ◊

This definition says that given the malicious verifier, we can efficiently construct the corresponding simulator. The transformation Y guarantees that if $\mathbf{V}^*$ is p.p.t., then so is $\mathbf{S} = Y(\mathbf{V}^*)$.

1. *Show that the above definitions of zero knowledge are equivalent.*

   Hint: This equivalence relies on the auxiliary information present in the definitions. Without the auxiliary information, the equivalence may not hold.

Bonus Question 2. A weaker definition for zero-knowledge *(5 points)*

As discussed in class, there are several relaxations of zero-knowledge. We saw one in class (honest verifier ZK). Another relaxation is witness indistinguishable proofs*, which is defined below.*

Definition (Witness Indistinguishability w.r.t Auxiliary Information)**.** *Let $(\mathbf{P}, \mathbf{V})$ be an interactive proof system for an* NP *language* L *with relation R_{L}, where both the prover and verifier are p.p.t. We say that the proof system satisfies witness indistinguishability if for every (possibly malicious) p.p.t. verifier $\mathbf{V}^*$ and polynomial p_1, for every distinguisher $\mathcal{D}$, there exists a negligible function μ such that for every $x \in \mathsf{L}_{\text{yes}}$, every w_1, w_2 such that $(x, w_1) \in R_{\mathsf{L}}$ and $(x, w_2) \in R_{\mathsf{L}}$, and every $z \in \{0,1\}^{p_1(|x|)}$ (note that z can depend on w_1, w_2),*

$$\Pr\left[\mathbf{D}^*\left(\text{view}\langle \mathbf{P}(w_1), \mathbf{V}^*(z)\rangle(x)\right) = 1\right] - \Pr\left[\mathbf{D}^*\left(\text{view}\langle \mathbf{P}(w_2), \mathbf{V}^*(z)\rangle(x)\right) = 1\right] \leq \mu(|x|)$$

where the probabilities are taken over the randomness used by $\mathbf{P}, \mathbf{V}^*$ and $\mathbf{D}^*$. ◊

Note that the zero-knowledge property implies witness indistinguishability. Also, by a simple hybrid argument, one can show that witness indistinguishable proofs can be repeated in parallel. Therefore, we have three-round WI proofs for NP*.*

1. *In class, we attempted to construct a zero-knowledge protocol for* SAT*, and there were some issues. Construct a witness-indistinguishable proof for* SAT*, or some other* NP-complete *language (other than* GraphHam *and* 3COL*). Your protocol should not involve a reduction to* GraphHam *or* 3COL*.*

[Bar01] Boaz Barak. How to Go Beyond the Black-Box Simulation Barrier. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*, pages 106–115. IEEE Computer Society, 2001.

[BLV04] Boaz Barak, Yehuda Lindell, and Salil P. Vadhan. Lower Bounds for Non-Black-Box Zero Knowledge. *IACR Cryptol. ePrint Arch.*, page 226, 2004.

[GKR15] Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. Delegating Computation: Interactive Proofs for Muggles. *J. ACM*, 62(4), sep 2015.

[GO94] Oded Goldreich and Yair Oren. Definitions and Properties of Zero-Knowledge Proof Systems. *J. Cryptol.*, 7(1):1–32, 1994.