OPRF Lower Bound

Jake Januzelli, Naman Kumar, Mike Rosulek

October 9, 2024

1 Definitions

Let $\mathsf{PRF} : \{0,1\}^\lambda \times \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}$ be a pseudorandom function with stretch $n \in \mathsf{poly}(\lambda)$. We define the OPRF Functionality $\mathcal{F}_{\mathsf{OPRF}}$ as follows.

OPRF Functionality $\mathcal{F}_{\mathsf{OPRF}}$

Inputs. $\mathcal{S}$ has input OPRF key $k \in \{0,1\}^\lambda$, $\mathcal{R}$ has input some $x \in \{0,1\}^{m(\lambda)}$ in the domain of the PRF.
Outputs. $\mathcal{R}$ gets $\mathsf{PRF}_k(x)$.

We further define the OT functionality as below.

OT Functionality $\mathcal{F}_{\mathsf{OT}}$

Inputs. $\mathcal{S}$ has input two strings $(m_0, m_1) \in \{0,1\}^{\mathsf{poly}(\lambda)}$ while receiver has a bit b.
Outputs. $\mathcal{R}$ gets m_b.

2 Proof of Insecurity of 'Trivial' PRF

We define $\mathsf{PRF}_k(x) = H(k||x)$ where $H : \{0,1\}^* \to \{0,1\}^{n(\lambda)}$ is a random oracle. Clearly this is a PRF; as the output of a random oracle, it is indistinguishable from a random function. We will prove the following theorem.

Theorem 2.1 (Communication complexity of OPRF, Perfect Completeness and Perfect Privacy)**.** *Let* PRF *be a pseudorandom function as defined above, and* $\mathcal{S}$ *and* $\mathcal{R}$ *be unbounded oracle TMs that have inputs as defined in* $\mathcal{F}_{\mathsf{OPRF}}$ *respectively. Then any protocol* Π_{OPRF} *which realizes* $\mathcal{F}_{\mathsf{OPRF}}$ *with perfect correctness and perfect privacy in the* $\mathcal{F}_{\mathsf{OT}}$*-hybrid model must have total communication complexity proportional to* $2^{m(\lambda)}$.

Brief Sketch. Our argument proceeds as follows.