OPRF Lower Bound

Jake Januzelli, Naman Kumar, Mike Rosulek

October 22, 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. Let $\mathcal{S}$ be an unbounded oracle TM and $\mathcal{R}$ be an oracle PPTM where both have access to the random oracle H.

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* $\mathcal{R}$ *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* $|X| = 2^{m(\lambda)}$.

Brief Sketch. Our argument proceeds as follows. Note that in order to evaluate the PRF at any point x, the oracle call $H(k||x)$ must be made. Clearly this oracle call cannot be made by the PPT receiver, since otherwise the receiver's view will consist of a polynomial-sized list of oracle queries to H which contains $k||x$ – this violates sender privacy as receiver learns k. Thus, this oracle call must be made by the sender.

Thus, the sender must make the oracle call $H(k||x)$. Furthermore, suppose there is some x for which the sender does not query $H(k||x)$. By the above argument it is clear that this call is not made by either party. However, if the receiver's input is x, then the receiver can only output the correct value of $H(k||x)$

with negligible probability, which contradicts perfect correctness of the protocol. It follows that $\mathcal{S}$ must make the oracle call $H(k||x)$ for each x.

Let Enc be an encoding algorithm such that $\mathsf{Enc} : x \times H(k||x) \mapsto F(x)$ and Dec be a decoding algorithm such that $\mathsf{Dec} : F(x) \times H(k||x) \mapsto X$. Let $\mathsf{Enc}(X)$ be $\mathcal{S}$'s input to $\mathcal{F}_{\mathsf{OT}}$. We require that $\Pr[\mathsf{Dec}(x, \mathsf{Enc}(x, H(k||x))) = H(k||x)] = 1$. It immediately follows that $|\mathsf{Enc}(X)| = |X| = O(2^m)$. The result follows from the trivial information-theoretic lower bound for OT.