Extending Oblivious Transfers with a Random Oracle

Joe Killian
NECI
4, Independence Way
Princeton, NJ 08540
U.S.A.

Abstract

We consider the problem of extending oblivious transfers: Given a small number of oblivious transfers "for free", can one implement a large number of oblivious transfers? Beaver has shown how to extend oblivious transfers given a one-way function. However, this protocol is inherently non-black box, and it was open whether one can extend oblivious transfers given a random black-box oracle. The nonexistence of such a method would have strong negative consequences for the reliability of black-box analyses.

For a passive sender and a malicious receiver, we give a very efficient protocol for extending oblivious transfer, based on a random oracle. After an initial setup between the sender and the receiver, exponentially many independent oblivious transfers may be realized by a single message from the sender to the receiver. Our method suggests a particularly fast heuristic for oblivious transfer that may be useful in some applications. We can use standard tricks to obtain an interactive protocol (with polynomial slowdown) that is secure against a malicious sender, but more efficient methods/analyses appear possible.

Joint work with Kobbi Nissim and Erez Petrank.