Single-Use Oblivious Transfer Combiners

Abstract

An oblivious transfer (OT) protocol allows a receiver to obtain one of two bits held by a sender without revealing its selection. An *OT combiner* securely implements OT by using oracle access to n OT candidates of which at most t may be insecure. It is known that OT combiners exist when $t < n/2$. However, known constructions either invoke each candidate multiple times or alternatively require t to be a very small fraction of n, even in the semi-honest security model.

In this work we study the goal of maximizing the security level of *single-use* OT combiners in the semi-honest model, namely OT combiners in which each candidate can only be invoked once. This question is motivated by scenarios in which each OT instance is implemented via a separate physical process that may leak information independent of other instances.

Our main result is a statistically secure single-use OT combiner which tolerates $t = n/2 - \tilde{O}(\log n)$ bad instances. We complement this by a negative result, showing that it is impossible to tolerate $t = n/2 - O(1)$ bad instances in this setting. More generally, given n OT instances, we construct single-use OT combiners where an adversary can corrupt the sender and t_S OT instances, or it can corrupt the receiver and t_R OT instances, such that $n - (t_S + t_R) = \tilde{O}(\log n)$.

Finally, we apply our positive result and (re-prove) the semi-honest completeness of (p, q)-*Weak-OT* [DKS99] (i.e. an OT which reveals the receiver choice bit to a corrupt sender with probability p and reveals both sender bits to a corrupt receiver with probability q), where $p + q < 1$. We significantly reduce the total number of (p, q)-WOT copies needed to implement one copy of OT.

Keywords: Single-use OT-combiners, Secret-sharing schemes, Semi-honest corruption, Adaptive security with erasures, Information-theoretic protocols, Weak Oblivious Transfer

(Joint work with Yuval Ishai, Amit Sahai and Jürg Wullschleger.)

References

[DKS99] Ivan Damgård, Joe Kilian, and Louis Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In Jacques Stern, editor, *EUROCRYPT*, volume 1592 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 1999. 1