Non-black-box Techniques in Cryptography

Boaz Barak

Princeton University

Abstract. In cryptography we typically prove the security of a scheme by reducing the task of breaking the scheme to some hard computational problem. This reduction usually done in a *black-box* fashion. By this we mean that there is an algorithm that can solve the hard problem given any black-box for breaking the scheme.

This lecture concerns exceptions to this rule: that is, schemes that are proven secure using a non-black-box reduction, that actually uses the code of a scheme-breaking attacker to construct a problem-solving algorithm. It turns out that such reductions can be used to obtain schemes with better properties that were known before. In fact, in some cases these non-black-box reductions can be obtain goals that were proven to be impossible to achieve when restricting to black-box reductions. In particular, we will present constructions of zero-knowledge protocols that are proven secure under various compositions [1, 2, 3].

We'll also discuss some of the limitations and open questions regarding non-black-box security proofs.

References

1. Barak, B.: How to go beyond the black-box simulation barrier. In: Proc. 42nd FOCS, IEEE (2001) 106–115
2. Pass, R.: Bounded-concurrent secure multi-party computation with a dishonest majority. In: Proc. 36th STOC, ACM (2004) 232–241
3. Barak, B., Sahai, A.: How to play almost any mental game over the net - concurrent composition using super-polynomial simulation. In: Proc. 46th FOCS, IEEE (2005)

D. Grigoriev, J. Harrison, and E.A. Hirsch (Eds.): CSR 2006, LNCS 3967, p. 1, 2006.