Cryptology ePrint Archive: Report 2011/324

On the Efficiency of Bit Commitment Reductions

Samuel Ranellucci and Alain Tapp and Severin Winkler and Jürg Wullschleger

Abstract: Two fundamental building blocks of secure two-party computation are oblivious transfer and bit commitment. While there exist unconditionally secure implementations of oblivious transfer from noisy correlations or channels that achieve constant rates, similar constructions are not known for bit commitment.

In this paper we show that any protocol that implements n instances of bit commitment with an error of at most 2^{-k} needs at least $\Omega(kn)$ instances of a given resource such as oblivious transfer or a noisy channel. This implies in particular that it is impossible to achieve a constant rate.

We then show that it is possible to circumvent the above lower bound by restricting the way in which the bit commitments can be opened. In the special case where only a constant number of instances can be opened, our protocol achieves a constant rate, which is optimal. Our protocol implements these restricted bit commitments from string commitments and is universally composable. The protocol provides significant speed-up over individual commitments in situations where restricted commitments are sufficient.

Category / Keywords: secure two-party computation, bit commitment, string commitment, oblivious transfer, noisy channel, information theory

Date: received 16 Jun 2011

Contact author: swinkler at ethz ch

Available formats: PDF | BibTeX Citation

Version: 20110617:072234 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]