Cryptology ePrint Archive: Report 2011/223

A Perfectly Binding Commitment Scheme Against Quantum Attacks

Zeng Bing and Chen Liang and Tang Xueming

Abstract: It's known that perfectly binding quantum computationally hiding commitment schemes can be constructed from any quantum one-way permutation. Since no quantum one-way permutations are known, it has been unknown by far whether we can get such a concrete commitment scheme. In this paper, we give a positive answer. Specifically, we present such a lattice-based commitment scheme, which is built from the results gained by Gentry et al.

Category / Keywords: secret-key cryptography / commitment scheme, lattice, quantum attack

Date: received 6 May 2011, last revised 22 May 2011

Contact author: zeng bing zb at gmail com