Cryptology ePrint Archive: Report 2011/599

Efficient Password-Based Authenticated Key Exchange from Lattices

Yi Ding and Lei Fan

Abstract: Protocols for password-based authenticated key exchange (PAKE) allow two users who share only a short, low-entropy password to agree on a cryptographically strong session key. One must ensure that protocols are immune to off-line dictionary attacks in which an adversary exhaustively enumerates all possible passwords in an attempt to determine the correct one. Recently Katz, et al. \cite{GK10} gave a new framework for realizing PAKE without random oracles, in the common reference string model.

In this paper, we instantiate the framework of \cite{GK10} under the lattices assumptions. Specifically, we modified the lattice-based approximate projective hashing introduced in \cite{KV09} and plug it into the framework of \cite{GK10}, and we prove our new PAKE is efficient and secure based on the security of GK's PAKE framework \cite{GK10} in the standard model.

Category / Keywords: public-key cryptography / lattice, PAKE

Date: received 5 Nov 2011, last revised 22 Dec 2011

Contact author: holmsding at gmail com