Cryptology ePrint Archive: Report 2013/092

Man-in-the-Middle Secure Authentication Schemes from LPN and Weak PRFs

Vadim Lyubashevsky and Daniel Masny

Abstract: We show how to construct, from any weak pseudorandom function, a 3-round symmetric-key authentication protocol that is secure against man-in-the-middle attacks. The construction is very efficient, requiring both the secret key and communication size to be only 3n bits long. Our techniques also extend to certain classes of randomized weak-PRFs, chiefly among which are those based on the classical LPN problem and its more efficient variants such as Toeplitz-LPN and Ring-LPN. Building a man-in-the-middle secure authentication scheme from any weak-PRF resolves a problem left open by Dodis et al. (Eurocrypt 2012), while building a man-in-the-middle secure scheme based on any variant of the LPN problem solves the main open question in a long line of research aimed at constructing a practical light-weight authentication scheme based on learning problems, which began with the work of Hopper and Blum (Asiacrypt 2001).

Category / Keywords: secret-key cryptography / authentication schemes, LPN, HB authentication,weak-PRFs

Date: received 20 Feb 2013, last revised 11 Mar 2013

Contact author: lyubash at di ens fr