Lyubashevsky, Vadim; **Masny, Daniel**

Man-in-the-middle secure authentication schemes from LPN and weak PRFs. (English)

Zbl 1316.94102

Canetti, Ran (ed.) et al., Advances in cryptology – CRYPTO 2013. 33rd annual cryptology conference, Santa Barbara, CA, USA, August 18–22, 2013. Proceedings, Part II. Berlin: Springer (ISBN 978-3-642-40083-4/pbk). Lecture Notes in Computer Science 8043, 308-325 (2013).

Summary: 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 and involving only one call to the weak-PRF. 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 an efficient man-in-the-middle secure authentication scheme from any weak-PRF resolves a problem left open by *Y. Dodis* et al. [Eurocrypt 2012, Lect. Notes Comput. Sci. 7237, 355–374 (2012; Zbl 1297.94117)]. 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 *N. J. Hopper* and *M. Blum* [Asiacrypt 2001, Lect. Notes Comput. Sci. 2248, 52–66 (2001; Zbl 1062.94549)].

For the entire collection see [Zbl 1270.94006].

MSC:

94A62 Authentication, digital signatures and secret sharing

Keywords:

weak pseudorandom function; 3-round symmetric-key authentication protocol; learning parity with noise (LPN) problem

Software:

PRESENT

Full Text: DOI