**Kiltz, Eike**; **Pietrzak, Krzysztof**; **Cash, David**; **Jain, Abhishek**; **Venturi, Daniele**
**Efficient authentication from hard learning problems.** (English) Zbl 1281.94083
Paterson, Kenneth G. (ed.), Advances in cryptology – EUROCRYPT 2011. 30th annual international conference on the theory and applications of cryptographic techniques, Tallinn, Estonia, May 15–19, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-20464-7/pbk). Lecture Notes in Computer Science 6632, 7-26 (2011).

Summary: We construct efficient authentication protocols and message-authentication codes (MACs) whose security can be reduced to the learning parity with noise (LPN) problem.

Despite a large body of work – starting with the HB protocol of *N. J. Hopper* and *M. Blum* in 2001 [ASIACRYPT 2001. Lect. Notes Comput. Sci. 2248, 52–66 (2001; Zbl 1062.94549)] – until now it was not even known how to construct an efficient authentication protocol from LPN which is secure against man-in-the-middle (MIM) attacks. A MAC implies such a (two-round) protocol.

For the entire collection see [Zbl 1214.94003].

**MSC:**

94A62 Authentication, digital signatures and secret sharing



**Software:**

HB-MP

**Full Text:** DOI