**Guo, Qian**; **Johansson, Thomas**; **Löndahl, Carl**

**Solving LPN using covering codes.** (English) Zbl 1306.94059

Sarkar, Palash (ed.) et al., Advances in cryptology – ASIACRYPT 2014. 20th international conference on the theory and application of cryptology and information security, Kaoshiung, Taiwan, R.O.C., December 7–11, 2014. Proceedings, Part I. Berlin: Springer (ISBN 978-3-662-45610-1/pbk). Lecture Notes in Computer Science 8873, 1-20 (2014).

Summary: We present a new algorithm for solving the LPN problem. The algorithm has a similar form as some previous methods, but includes a new key step that makes use of approximations of random words to a nearest codeword in a linear code. It outperforms previous methods for many parameter choices. In particular, we can now solve instances suggested for 80-bit security in cryptographic schemes like HB variants, LPN-C and Lapin, in less than $2^{80}$ operations.

For the entire collection see [Zbl 1301.94003].

**MSC:**

94A60 Cryptography
94B75 Applications of the theory of convex sets and geometry of numbers (covering radius, etc.) to coding theory



**Keywords:**

Learning Parity with Noise (LPN)

**Full Text:** DOI Link