Zhang, Bin; **Jiao, Lin**; **Wang, Mingsheng**

Faster algorithms for solving LPN. (English) Zbl 1347.94064

Fischlin, Marc (ed.) et al., Advances in cryptology – EUROCRYPT 2016. 35th annual international conference on the theory and applications of cryptographic techniques, Vienna, Austria, May 8–12, 2016. Proceedings. Part I. Berlin: Springer (ISBN 978-3-662-49889-7/pbk; 978-3-662-49890-3/ebook). Lecture Notes in Computer Science 9665, 168-195 (2016).

Summary: The LPN problem, lying at the core of many cryptographic constructions for lightweight and post-quantum cryptography, receives quite a lot attention recently. The best published algorithm for solving it at Asiacrypt 2014 [*Q. Guo* et al., Lect. Notes Comput. Sci. 8873, 1–20 (2014; Zbl 1306.94059)] improved the classical BKW algorithm by using covering codes, which claimed to marginally compromise the 80-bit security of HB variants, LPN-C and Lapin. In this paper, we develop faster algorithms for solving LPN based on an optimal precise embedding of cascaded concrete perfect codes, in a similar framework but with many optimizations. Our algorithm outperforms the previous methods for the proposed parameter choices and distinctly break the 80-bit security bound of the instances suggested in cryptographic schemes like HB^{+}, $HB^{\#}$, LPN-C and Lapin.

For the entire collection see [Zbl 1339.94004].

MSC:

94A60 Cryptography

Keywords:

Learning Parity with Noise (LPN); Blum-Kalai-Wasserman (BKW) algorithm; perfect code; Hopper-Blum (HB) protocol; Lapin

Full Text: DOI