Cryptology ePrint Archive: Report 2011/120

Faster 2-regular information-set decoding

Daniel J. Bernstein and Tanja Lange and Christiane Peters and Peter Schwabe

Abstract: Fix positive integers B and w. Let C be a linear code over F_2 of length Bw. The 2-regular-decoding problem is to &#64257;nd a nonzero codeword consisting of w length-B blocks, each of which has Hamming weight 0 or 2. This problem appears in attacks on the FSB (fast syndrome-based) hash function and related proposals. This problem differs from the usual information-set-decoding problems in that (1) the target codeword is required to have a very regular structure and (2) the target weight can be rather high, so that there are many possible codewords of that weight.

Augot, Finiasz, and Sendrier, in the paper that introduced FSB, pre- sented a variant of information-set decoding tuned for 2-regular decoding. This paper improves the Augot–Finiasz–Sendrier algorithm in a way that is analogous to Stern's improvement upon basic information-set decoding. The resulting algorithm achieves an exponential speedup over the previous algorithm.

Category / Keywords: secret-key cryptography / Information-set decoding, 2-regular decoding, FSB, binary codes

Date: received 9 Mar 2011

Contact author: tanja at hyperelliptic org

Available formats: PDF | BibTeX Citation

Version: 20110310:022616 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]