Cryptology ePrint Archive: Report 2011/502

Wild McEliece Incognito

Daniel J. Bernstein and Tanja Lange and Christiane Peters

Abstract: The wild McEliece cryptosystem uses wild Goppa codes over finite fields to achieve smaller public key sizes compared to the original McEliece cryptosystem at the same level of security against all attacks known. However, the cryptosystem drops one of the confidence-inspiring shields built into the original McEliece cryptosystem, namely a large pool of Goppa polynomials to choose from.

This paper shows how to achieve almost all of the same reduction in key size while preserving this shield. Even if support splitting could be (1) generalized to handle an unknown support set and (2) sped up by a square-root factor, polynomial-searching attacks in the new system will still be at least as hard as information-set decoding.

Furthermore, this paper presents a set of concrete cryptanalytic challenges to encourage the cryptographic community to study the security of code-based cryptography. The challenges range through codes over F_2, F_3,..., F_32, and cover two different levels of how much the wildness is hidden.

Category / Keywords: public-key cryptography / McEliece cryptosystem, Niederreiter cryptosystem, Goppa codes, wild Goppa codes, list decoding

Publication Info: expanded version

Date: received 15 Sep 2011, last revised 15 Sep 2011

Contact author: c p peters at mat dtu dk