Cryptology ePrint Archive: Report 2011/179

Compact McEliece keys based on Quasi-Dyadic Srivastava codes

Edoardo Persichetti

Abstract: The McEliece cryptosystem is one of the few systems to be considered secure against Quantum attacks. The original scheme is built upon Goppa codes and produces very large keys, hence latest research has focused mainly on trying to reduce the public key size. Previous proposals tried to replace the class of Goppa codes with other families of codes, but this revealed to be an insecure choice. In this paper we introduce a construction based on Generalized Srivastava codes, a large class which include Goppa codes as a special case, that allows relatively short public keys without being vulnerable to known structural attacks.

Category / Keywords: public-key cryptography / Coding Theory, McEliece

Date: received 6 Apr 2011, last revised 27 Nov 2011

Contact author: e persichetti at math auckland ac nz