Code-based cryptography with error-correcting pairs

Ruud Pellikaan
Dept. Mathematics and Computing Science. Technical University of Eindhoven (Netherlands)
g.r.pellikaan@tue.nl

Abstract

First we will review elementary facts of error-correcting codes and their decoding. Then we will explain how to decode efficiently those codes that have an error-correcting pair [3, 4]. Generalities of one-way functions and public key crypto systems will be given. The McEliece public crypto system is based on the hardness of decoding a general code [2]. Finally we consider the question of the one-way-ness of error-correcting pair function [1, 5].

Keywords
McEliece public crypto system, error-correcting pair

References

[1] I. Márquez-Corbella and R. Pellikaan: "Error-correcting pairs for a public-key cryptosystem". Preprint arXiv:1205.3647 (2012).

[2] R. A. McEliece: "A public-key cryptosystem based on algebraic coding theory". DSN Progress Report 4244, 114-116 (1978).

[3] R. Pellikaan: "On decoding by error location and dependent sets of error positions". Discrete Math. 106107, 369-381 (1992).

[4] R. Pellikaan: "On the existence of error-correcting pairs". Statistical Planning and Inference 51, 229-242 (1996).

[5] R. Pellikaan and I. Márquez-Corbella "Error-correcting pairs for a public-key cryptosystem". J. Phys.: Conf. Ser. 855, 012032 (2017).