Is it hard to retrieve an error-correcting pair?

Irene Márquez-Corbella * and Ruud Pellikaan †

Applications of Computer Algebra, 1 Aug 2016, Kassel
Computer Algebra in Coding Theory and Cryptography
Booklet of abstracts, p. 234-236, 2016

Abstract

Code-based cryptography is an interesting alternative to classic number-theory PKC since it is conjectured to be secure against quantum computer attacks. Many families of codes have been proposed for these cryptosystems. One of the main requirements is having high performance $t$-bounded decoding algorithms which is achieved in the case the code as a $t$-error-correcting pair. The class of codes with a $t$-ECP is proposed for the McEliece cryptosystem. The hardness of retrieving the $t$-ECP for a given code is considered. To this end we have to solve a large system of bilinear equations. Two possible induction procedures are considered, one for sub/super ECP’s and one by puncturing/shortening. In both procedures in every step only a few bilinear equations need to be solved.

1 Introduction

Error-correcting pairs (ECP) were introduced and studied in [4, 7, 8], as a general algebraic method of decoding linear codes. It was shown that an $[n, n - 2t, 2t + 2]$ code has a $t$-error correcting pair if and only if it is a Generalized Reed-Solomon code [6]. The concept of an ECP is instrumental

---

* CryptULL, Universidad de La Laguna, Tenerife, E-mail: irene.marquez-corbella@inria.fr
† Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands. E-mail: g.r.pellikaan@tue.nl
in the polynomial attack of the McEliece cryptosystem that uses algebraic geometry codes [2].

The class of codes with a $t$-ECP is proposed for the McEliece cryptosystem [5]. The hardness of retrieving the $t$-ECP for a given code is considered. To this end we have to solve a large system of bilinear equations [3, 1]. Two possible induction procedures are considered, one for sub/super ECP’s and one by puncturing/shortening. In both procedures in every step only a few bilinear equations need to be solved.

Let $P(n, t, q)$ be the collection of pairs $(A, B)$ such that there exist a positive integer $m$ and a pair $(A, B)$ of $F_{q^m}$-linear codes of length $n$ that satisfy the conditions E.2, E.3, E.5 and E.6

Let $C$ be the $F_q$-linear code of length $n$ that is the subfield subcode that has the elements of $A \ast B$ as parity checks

$$C = F_q^n \cap (A \ast B)^\perp$$

Then the minimum distance of $C$ is at least $2t + 1$ and $(A, B)$ is a $t$-ECP for $C$

Let $F(n, t, q)$ be the collection of $F_q$-linear codes of length $n$ and minimum distance $d \geq 2t + 1$

Consider the following map

$$\varphi(n, t, q) : P(n, t, q) \longrightarrow F(n, t, q)$$

$$(A, B) \ maps to C$$

The question is whether this map is a one-way function.

We treat the entries of the generator matrices of the the pair of codes $(A, B)$ as variables $X_{ij}$ and $Y_{ij}$. The condition $(A \ast B) \perp C$ becomes a system of bilinear equations. We will apply the $F_5$-method to find Gröbner basis for a solution [3, 1]. The puncturing and shortening procedure that was used in [6] will reduce the number of variables.
References


