Is it hard to retrieve an error-correcting pair?

Irene Márquez-Corbella, Ruud Pellikaan

Is it hard to retrieve an error-correcting pair?

Irene Márquez-Corbella and Ruud Pellikaan

Dept. of Mathematics, Statistics and O. Research, University of La Laguna, Spain.
irene.marquez.corbella@ull.es
Dept. of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands. g.r.pellikaan@tue.nl

Code-based cryptography is an interesting alternative to classic number-theory Public-Key Cryptosystems (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 has a t-error-correcting pair (ECP). 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 Notation and Prerrequisites

By $\mathbb{F}_q$, where q is a prime power, we denote a finite field with q elements. An $[n,k]$ linear code $\mathscr{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. We will denote the length of $\mathscr{C}$ by $n(\mathscr{C})$, its dimension by $k(\mathscr{C})$ and its minimum distance, $d(\mathscr{C})$.

Given two elements $\mathbf{a}$ and $\mathbf{b}$ on $\mathbb{F}_q^n$, the *star multiplication* is defined by coordinatewise multiplication, that is, $\mathbf{a}*\mathbf{b} = (a_1b_1,\ldots,a_nb_n)$. Then, $A*B$ is the code in $\mathbb{F}_q^n$ generated by $\{\mathbf{a}*\mathbf{b} \mid \mathbf{a}\in A \text{ and } \mathbf{b}\in B\}$.

The *standard inner multiplication* of $\mathbf{a}$ and $\mathbf{b}$ on $\mathbb{F}_q^n$ is defined by $\mathbf{a}\cdot\mathbf{b} = \sum_{i=1}^n a_ib_i$. Now $A\perp B$ if and only if $\mathbf{a}\cdot\mathbf{b}=0$ for all $\mathbf{a}\in A$ and $\mathbf{b}\in B$.

Definition 1 *Let C be an $\mathbb{F}_q$-linear code of length n. The pair (A,B) of $\mathbb{F}_{q^m}$-linear codes of length n is called a t-error correcting pair (ECP) for C if the following properties holds:*

*E.*1 $(A*B)\perp C$,

*E.*2 $k(A) > t$,

*E.*3 $d(B^\perp) > t$,

*E.*4 $d(A)+d(C) > n$.

Broadly speaking: given a positive integer t, a t-ECP for a linear code $C\subseteq F_q^n$ is a pair of linear codes (A,B) satisfying that $A*B\subseteq C^\perp$ together with several

inequalities relating t and the dimensions and (dual) minimum distances of A, B and C. Furthermore note that if the fourth property (E.4) is replaced by the statements presented below then, again (A,B) is a t-ECP for C and the minimum distance of such linear code is at least $2t+1$.

E.5 $d(A^{\perp}) > 1$ or equivalently A is a non-degenerated code,

E.5 $d(A) + 2t > n$.

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 in the polynomial attack of the McEliece cryptosystem that uses algebraic geometry codes [2].

2 The McEliece PKC system using ECP's

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

Let C be the $\mathbb{F}_q$-linear code of length n that is the subfield subcode that has the elements of $A * B$ as parity checks

$$C = \mathbb{F}_q^n \cap (A * B)^{\perp}$$

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

Let $\mathscr{F}(n,t,q)$ be the collection of $\mathbb{F}_q$-linear codes of length n and minimum distance $d \geq 2t+1$.

Consider the following map

$$\begin{array}{rccc} \varphi_{(n,t,q)}: & \mathscr{P}(n,t,q) & \longrightarrow & \mathscr{F}(n,t,q) \\ & (A,B) & \longmapsto & C \end{array}$$

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 $(A*B) \perp C$ 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

[1] M. Bardet, J.-C. Faugère, B. Salvy, and P.-J. Spaenlehauer. On the complexity of solving quadratic boolean systems. *CoRR*, abs/1112.6263, 2011.

[2] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan. Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes. *ArXiv e-prints 1409.8220*, September 2014.

[3] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree $(1,1)$: algorithms and complexity. *J. Symbolic Comput.*, 46(4):406–437, 2011.

[4] R. Kötter. A unified description of an error locating procedure for linear codes. In *Proceedings of Algebraic and Combinatorial Coding Theory*, pages 113–117. Voneshta Voda, 1992.

[5] I. Márquez-Corbella and R. Pellikaan. Error-correcting pairs for a public-key cryptosystem. *ArXiv e-prints 1205.3647v1*, 2012.

[6] Irene Márquez-Corbella and Ruud Pellikaan. A characterization of mds codes that have an error correcting pair. *Finite Fields Appl.*, 40(C):224–245, July 2016.

[7] R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.*, 106–107:369–381, 1992.

[8] R. Pellikaan. On the existence of error-correcting pairs. *Statistical Planning and Inference*, 51:229–242, 1996.