Cryptanalysis of some McEliece Variants based on Monomial Codes

Vlad-Florin Drăgoi Andreea Szöcs

Aurel Vlaicu University of Arad, Romania

McEliece variant based on Self-dual monomial codes The McEliece public-key encryption scheme has gained a lot of attention during the last decades. One of the recent proposals adopts self-dual monomial codes [4] instead of binary Goppa codes. This variant presents a lot of similarities with older schemes, such as Sidenlnikov's cryptosystem based on Reed-Muller codes [7] and the McEliece variant based on polar codes [6]. Since these were successfully cryptanalysed ([2, 5, 1]), in this document, we turn our head toward different techniques that might threaten the security of the scheme in [4]. We will give here recently published results from [3] as well as new directions in completing the security analysis of a larger class of self-dual monomial codes. Let us point out some advantages of self-dual monomial codes when used in a cryptographic context.

- the hull of the code equals the code itself, and hence, generic algorithms for solving the code equivalence problem are unfit for this scheme;
- as we shall see, even for a more structured configuration of the monomial set I defining the code, applying square code and shortening only reduces the code equivalence problem to the most difficult instance of the code equivalence problem on the Reed-Muller codes;
- there is an exponential number of sets I to be considered and hence an exponential number of instances of the code equivalence problem to be solved;
- different choices of I give different permutation groups for $\mathscr{C}(I)$ and, implicitly, different numbers and structures of minimum weight codewords. Again, for more structured choices of I, the code spanned by the minimum weight codewords is equivalent to a certain Reed-Muller code for which the attacks such as [2] do not manage to reduce the complexity of [5].

Self-dual weakly decreasing monomial codes Monomial codes are linear binary codes $\mathscr{C}(I)$ defined by a set of monomials $I \subset \mathcal{M}_{[m]}$ by means of an evaluation function $\mathscr{C}(I) = \mathrm{Span}_{\mathbb{F}_2}(\{\mathsf{ev}(f) \mid f \in I\}) \subseteq \mathbb{F}_2^n$, where $\mathcal{M}_{[m]}$ is the subset of all monomials from the ring of polynomials $\mathbb{F}_2[x_0, \ldots, x_{m-1}]/(x_0^2 - x_0, \ldots, x_{m-1}^2 - x_{m-1})$. (see [1] for details). When the monomials in the set I satisfy the partial order relation $f \preceq_{\mathrm{w}} g \Leftrightarrow f|g$, then the monomial code $\mathscr{C}(I)$ is called weakly decreasing. Famous families of codes, e.g., Reed-Muller and polar codes, are known to posses this order relation. Duality properties mainly resume, in the case of weakly decreasing monomial codes, to the multiplicative complement of a monomial, $\check{g} = x_0 \ldots x_{m-1}/g$. More precisely, if we have that $\forall f \in I,\ \check{f} \notin I$ then $\mathscr{C}(I)$ is weakly self-dual, or self-dual (depending on its dimension). A construction of self-dual monomial codes is proposed in the McEliece scheme in [4]. We shall propose a classification of all weakly decreasing self-dual monomial codes and analyse the security of some sub-families of codes, including the particular case from [4]. For that, let $I_{\leq r} = \{f \in \mathcal{M}_{[m]} \mid \deg(f) \leq r\}$. The first class, which was partially cryptanalysed in [3] is defined by $I = I_{\leq \frac{m}{2}-1} \cup J$ where a) $\exists i \in [m]$ such that $J = x_i I_{\leq \frac{m}{2}-1}$; b) $\nexists i \in [m]$ such that $J = x_i I_{\leq \frac{m}{2}-1}$. The second class is defined by I with $I_{\leq \frac{m}{2}-1} \not\subset I$, such that a) $\exists i \in [m]$ s.t. $x_i \notin I$; b) $I_1 \subset I$.

Properties of the first class of weakly decreasing self-dual monomial codes One of the key ingredients in analysing the security of the McEliece variant [4] is to clearly understand what the square of a weakly decreasing self-dual monomial code is. The following result comes from [3].

$$\left(\mathscr{C}(I)^2\right)^{\perp} = \begin{cases} \mathscr{C}(\{\mathbf{1}, x_i\}) & \text{if } \exists i, \forall f \in J, x_i | f \\ \mathscr{C}(\{\mathbf{1}\}) & \text{if not} \end{cases} \tag{1}$$

Based on this result, a possible key recovery attack is proposed. More precisely, we can identify, up to a permutation, a variable x_i when $I = I_{\leq \frac{m}{2}-1} \cup x_i I_{\leq \frac{m}{2}-1}$. With this information at hand, we can demonstrate that, if we shorten the code on the support of the evaluation of $1 + x_i$, our key recovery problem is equivalent

to a key recovery problem on the $\mathscr{R}(\frac{m}{2}-1, m-1)$ which is the hardest instance to solve of Sidelnikov's cryptosystem. Hence, even though the choice $I = I_{\leq \frac{m}{2}-1} \cup x_i I_{\leq \frac{m}{2}-1}$ leaks information about x_i, we are still left with a difficult problem to solve. One of the ingredients provided in our approach was a characterization of the permutation group of the code $\mathscr{C}(I)$ with $I = I_{\leq \frac{m}{2}-1} \cup x_i I_{\leq \frac{m}{2}-1}$. This particular choice turned out to posses a group of automorphisms larger than the general affine group.

The second case, when there is no variable x_i s.t. $x_i | f$ for all $f \in J$, the things seem even more complicated. A generic approach could be imagined, a strategy we are currently working on, in which information about the minimum weight codewords is used. The difficulty of this approach is two-fold : i) the time complexity of retrieving a minimum weight codeword is roughly $e^{c\sqrt{n}}$ (where c is a constant); ii) we do not yet have a characterisation of the structure of the minimum weight codewords of such codes. However, we have proved in [3] that there is an efficient distinguisher for this class of codes.

Second class of weakly-decreasing self dual monomial codes At present, we are working on this second class of monomial codes. A yet unpublished result is a key recovery attack for the second subclass of this family. It is based on the following two arguments:

- when a variable is missing from I, one can efficiently find a permutation $\pi_i \in S_n$ such that $\mathscr{C}(\mathcal{M}_{[m]\setminus\{i\}})^{\pi_i} = \mathscr{C}(\mathcal{M}_{[m-1]})$;
- if $I = \mathcal{M}_{[m-1]}$, then the block matrix $\left[\boldsymbol{I}|\boldsymbol{I}\right]$ is a generator matrix for the code $\mathscr{C}(I)$ with I evaluated over $\mathbb{F}_2^m$.

With these at hand, a simple and efficient method for solving the code equivalence problem in this particular case can be deduce. The procedure works as follows: 1) Search a small basis for the permuted code (using vectors of weight 2 which are evaluation of all the elements in the orbit of $T(m,2) \cdot \check{x_i}$); 2) Compute a permutation that maps the small basis from step 1) to the basis $\left[\boldsymbol{I}|\boldsymbol{I}\right]$. Both the first and the second step can be efficiently implemented.

The permutation group question There is at least one theoretical question that could help us better understand the difficulty of the key recovery problem for the McEliece based on weakly decreasing self-dual monomial codes: What is the permutation group of these codes? Even if for particular sub-families the answer was given, no results are known for the vast majority. Answering this question could lead us to understanding the structure of the minimum weight codewords. It also has a second practical application, i.e., it can help in the decoding process (algorithms for decoding these codes in general are not known, except, for instance, maximum-likelihood decoding).

References

[1] Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich. Cryptanalysis of the McEliece public key cryptosystem based on polar codes. In *Post-Quantum Cryptography2016*, Lecture Notes in Comput. Sci., Fukuoka, Japan, February 2016.

[2] Ivan V. Chizhov and Mikhail A. Borodin. Effective attack on the McEliece cryptosystem based on Reed-Muller codes. *Discrete Math. Appl.*, 24(5):273–280, 2014.

[3] Vlad-Florin Drăgoi and Andreea Szöcs. Structural properties of self-dual monomial codes with application to code-based cryptography. In Maura B. Paterson, editor, *Cryptography and Coding*, pages 16–41, Cham, 2021. Springer International Publishing.

[4] Pál Dömösi, Carolin Hannusch, and Géza Horváth. A cryptographic system based on a new class of binary error-correcting codes. *Tatra Mountains Mathematical Publications*, 73(1):83–96, 2019.

[5] Lorenz Minder and Amin Shokrollahi. Cryptanalysis of the Sidelnikov cryptosystem. In *Advances in Cryptology - EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Comput. Sci.*, pages 347–360, Barcelona, Spain, 2007.

[6] Sujan Raj Shrestha and Young-Sik Kim. New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography. In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, pages 368–372. IEEE, 2014.

[7] Vladimir Michilovich Sidelnikov. A public-key cryptosytem based on Reed-Muller codes. *Discrete Math. Appl.*, 4(3):191–207, 1994.