Structural attack on quasy-cyclic SSAG-code-based McEliece cryptosystems

Mathieu Lhotel

December 3, 2021

In the area of post-quantum cryptography, public key cryptography using linear codes looks promising. The first such system was introduced by McEliece in 1978, using binary classical Goppa codes. The main problem of this scheme is that the size of the public key is to large for certain practical use cases. Many propositions were made in order to correct this, mostly by considering codes with additional structure, e.g. quasi-cyclic codes. Moreover, replacing classical Goppa codes, which are defined over the line, by their natural generalization, AG-codes on curves, can also help in providing more flexibility.

However, recent works from Couvreur, Marquez-Corbella and Pellikaan (2014) broke McEliece cryptosystems based on raw AG-codes on arbitrary genus curves. So, in the same way that classical Goppa codes can be seen as subfield subcodes of GRS codes, this leads to more specifically consider subfield subcodes of AG-codes (SSAG in short), for which there are only few propositions to date.

The present work is a generalization of the structural attack proposed by Barelli (2018), which concerned quasi-cyclic SSAG-codes on Kummer coverings of the projective line. Her main idea was to use the structure of the invariant subcode in order to retrieve the secrete structure of the public code. The weak point of this attack is that it mainly uses the fact that the quotient curve has genus zero, which gives little hope for potential extentions to other coverings.

Our work takes up similar ideas, but without using the genus of the quotient curve. Therefore, were are able to apply our procedure to any structured SSAG-code on a Galois covering of a curve which is defined by a separated variables equation. As a consequence, the security of the underlying scheme reduces to the security of the much smaller invariant code, implying a smart choice of the system parameters in order to keep a good security level.