Public key cryptosystems based on algebraic geometry codes

Ruud Pellikaan*

Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven

Abstract

This is a report on the McEliece public key cryptosystem based on algebraic geometry codes. In [3, 4] it is explained how a representation $(\mathcal{Y}, \mathcal{Q}, F)$ is retrieved efficiently from a generator matrix of the algebraic geometry code $\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$ for a given curve $\mathcal{X}$, an n-tuple $\mathcal{P}$ of points on the curve and a divisor E. This result is not sufficient to obtain a polynomial attack on the public key cryptosystem based on these codes. In [1] a polynomial time attack is given using the idea of an error correcting pair [5]. It runs in $O(n^4)$ elementary operations in $\mathbb{F}_q$, where n denotes the code length. Compared to previous attacks, it allows to recover a decoding algorithm for the public key even for codes from high genus curves.
Recently the attack was extended to subcodes of algebraic geometry codes [2].
The problem for subfield subcodes of algebraic geometry codes is still open.

Joint work with Alain Couvreur, Irene Márquez-Corbella, Edgar Martínez-Moro and Diego Ruano. See [1, 3, 4].

References

[1] A. Couvreur and I. Marquez–Corbella and R. Pellikaan, "A polynomial time attack against algebraic geometry code based public key cryptosystems", ISIT 2014, pp. 1446, 2014.

[2] A. Couvreur and I. Marquez–Corbella and R. Pellikaan, "Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes", 4ICMCTA, 2014.

[3] Márquez-Corbella, I. and Martínez-Moro, E. and Pellikaan, R. "On the unique representation of very strong algebraic geometry codes", Designs, Codes and Cryptography 70, pp. 215-230, 2014.

[4] Márquez-Corbella, I. and E. Martínez-Moro and R. Pellikaan and D. Ruano, "Computational aspects of retrieving a representation of an algebraic geometry code", Journ. Symb. Comput. 64, pp. 67–87, 2014.

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

*g.r.pellikaan@tue.nl