Index Calculus Attacks on Hyperelliptic Jacobians with Effective Endomorphisms

Sulamithe Tsakou

Laboratoire MIS, Université de Picardie Jules Verne, Amiens, France
{sulamithe.tsakou@u-picardie.fr

The security of many existing cryptographic systems relies on the difficulty of solving the discrete logarithm problem (DLP) over a finite field. For a generic group, we can solve this problem with many algorithms such as the baby-step-giant-step, the Pollard-rho or the Pohlig-Hellman algorithm. For a group with known structure, we use the index calculus algorithm to solve the discrete logarithm problem. Then, the DLP on the Jacobian of a hyperelliptic curve defined over a finite field IFqn with $n > 1$ are subject to index calculus attacks. After having chosen a convenient factor basis, the index calculus algorithm has three steps : the decomposition step in which we decompose a random point in the factor basis, the linear algebra step where we solve a matricial equation and the descent phase in which the discrete logarithm is deduced. The complexity of the algorithm crucially depends on the size of the factor basis, since this determines the probability for a point to be decomposed over the base and also the cost of the linear algebra step. Faugère et al [1] exploit the 2-torsion point of the curve to reduce the size of the factor basis and then improve the complexity of the index calculus algorithm. In a similar manner, we exploit the endomorphism of the Jacobian to reduce the size of the factor base for certain families of ordinary elliptic curves and genus 2 hyperelliptic Jacobians defined over finite fields. This approach adds an extra cost when performing operation on the factor basis, but our benchmarks show that reducing the size of the factor base allows to have a gain on the total complexity of index calculus algorithm with respect to the generic attacks.

References

1. Faugère, J.-C., Huot, L., Joux, A., Renault, G., Vitse, V, Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus. In: Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2014, Proceedings, Vol. 8441. Lecture Notes in Computer Science. Springer. 2014, pp. 40-57.