**Selection of primes in the KLPT algorithm for construction of fast isogeny**

Yasushi Takahashi 1,2, Yuta Kambe 2,3, Masaya Yasuda 2, Kazuhiro Yokoyama 2

FUJITSU LTD., 4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki, Kanagawa, Japan, t-yasuhi@fujitsu.com

Rikkyo University, 3-34-1, Nishiikebukuro, Toyosima-ku, Tokyo, Japan, {yasuda,kazuhiro}@rikkyo.ac.jp

Sugakubunka Ltd., 5F, Musashibiru, 7-4-4, Nishishinjuku, Shinjuku-ku, Tokyo, Japan, yuta.kambe.math@gmail.com

---

**Background**

Isogeny cryptosystems are known as one of the candidates for post-quantum cryptography. Especially, KLPT-based isogeny cryptosystems (such as [1]) have recently proposed. These cryptosystems use KLPT algorithm [2] which computes an ideal that is isomorphic to the given ideal and has a smooth norm and isogeny construction which computes an isogeny corresponding with an smooth ideal. However, it has not been sufficiently speeded up since there are few implementations and improvements for the KLPT algorithm.

**Our Purpose and Improvement**

In isogeny cryptosystems, the main steps are the KLPT algorithm step and the isogeny construction step (refer to Fig.1). Our purpose is to speed up the isogeny construction step in the cryptosystems by modifying the KLPT algorithm. In the KLPT algorithm step, for an input ideal, output is an ideal that is isomorphic to it and has a smooth norm. In the isogeny construction step, the ideal output by the KLPT algorithm is used as input to calculate an isogeny with a smooth degree corresponding to the ideal. In that step, let $\ell$ be a prime factor of the norm of the input ideal, then we compute the extension basis of $E[\ell]$ over $F_p$. So, in order to reduce this computational cost, we improve the KLPT algorithm so that its output is an ideal with a smaller size of its extension basis.

KLPT algorithm computes an element $\beta$ with a smooth norm in a maximal order to construct the output ideal with a smooth norm. Therefore, we will improve the KLPT algorithm to compute $\beta$ with the norm composed by the prime $\ell$'s for which the extension degree of $E[\ell]$ over $F_p$ is small.

**Experiments**

Based on [3], we implemented our modified KLPT algorithm with the above improvement. Here, we fix the starting curve to $E/F_p$; $y^2 = x^3 + x$. Then, the value $\deg(E[\ell]/F_p)$ for each $\ell$ is also fixed, so this value can be precomputed. In this poster, we experimented using the lists of $\ell$'s not only sorted by $k := \deg(E[\ell]/F_p)$ but also $\ell k$ and $\ell k^2$ to find the appropriate sorting criteria. We used SageMath 9.2 and the following machine; Intel(R) Core(TM) i7-1185G7 3.00GHz, 16GB. For a prime $p$, we computed the list of $\ell$'s sorted by a criterion. And then, we execute KLPT algorithm using that list.

**Future Work**

In this poster, we only measured the computation time of the improved KLPT algorithm. Therefore, we will measure the time for isogeny construction when each criterion is used, and decide whether the criterion should be selected, considering the trade-off with the time of KLPT algorithm.

**References**

