The largest class group computation ever, and why it is useful for cryptography.

Ward Beullens

COSIC-imec, KU Leuven, Belgium

Recently, in joint work with Thorsten Kleinjung and Frederik Vercauteren, we computed the structure of the ideal class group of $\mathbb{Q}(\sqrt{-p})$, where p is a 152 digit prime. This computation took 52 core years of computing power. Our computation breaks the previous record from 2015, which computed the ideal class group of $\mathbb{Q}(\sqrt{-d})$, where d is the 130 digit integer $\lceil 10^{129}\pi \rceil$.

This computation is relevant for CSIDH, a cryptosystem that was recently proposed by Castryck et al. This cryptosystem uses the group action of the ideal class group $\mathsf{cl}(\mathcal{O})$, where $\mathcal{O} = \mathbb{Z}(\sqrt{-p})$, on the set $\mathcal{E}ll_p(\mathcal{O})$ of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$ with $\mathbb{F}_p$-endomorphism ring $\mathcal{O}$.

$$\begin{aligned} \star : \mathsf{cl}(\mathcal{O}) \times \mathcal{E}ll_p(\mathcal{O}) &\to \mathcal{E}ll_p(\mathcal{O}) \\ (\mathfrak{a}, E) &\mapsto E/E[\mathfrak{a}] \end{aligned}$$

It turns out that if the prime p is carefully crafted, this group action can be computed efficiently, and can be used to build a key exchange protocol.

Even though we know a set of generators of $\mathsf{cl}(\mathcal{O})$, the exact structure of the class group $\mathsf{cl}(\mathcal{O})$ is not known. Therefore, cryptographers are rather limited in what they can do with this group action. For example, it is not known how to uniformly sample elements from $\mathsf{cl}(\mathcal{O})$, or represent such elements uniquely. In our work, we solve this problem by computing the structure of the class group for a specific prime p proposed in the CSIDH paper. Hence, uniform sampling and unique representation of class group elements becomes feasible, which in turn makes it possible to build more cryptographic applications from the CSIDH action. In particular, we can instantiate an old signature scheme by Stolbunov. Given the output of our class group computation, this allowed us to implement the first practical isogeny-based signature scheme.

Kasteelpark Arenberg 10, 3001 Heverlee
ward.beullens@esat.kuleuven.be