AUSSOIS WINTER SCHOOL

17-22 MARCH 2019
Mattia Veroni

Supported by COINS, I attended the winter school at Aussois, named Maths of Public-Key Cryptography Winter School. The main topics of the talks were

- Lattice-based cryptography (50%);
- Isogeny based cryptography (25%);
- Discrete logarithm problem (25%).

I left on the morning of Sunday 17th in order to be there for the welcome dinner. Aussois is a commune in the Vanoise massif, in the Savoie department in the Auvergne-Rhône-Alpes region in south-eastern France. The village is on the border of France's first National Park, the Vanoise National Park.

The venue was not astonishing and represents the only negative point that I have to remark. Aussois is very hard to reach, especially from Trondheim. It took me 15 hours to go there and I had to spend an extra night in Turin due to the lack of connecting flights on my way back. The hotel was very old and the rooms quite dusty and very simply furnished. The conference room was large but not very practical, due to the lack of power outlets. The food was ok, good enough but nothing special. For the fees we had to pay, I would have expected an higher quality.

On the other hand, the talks were interesting and well given. The speakers/lecturers were top young researchers in the field of pre- and post-quantum cryptography. Among all the others, the most interesting speakers I had the chance to hear from were:

- Luca de Feo, who talked about isogeny graphs of elliptic curves in cryptography, with a particular focus on super singular isogeny graphs for post-quantum cryptography. The talk was long and consisted of a summary of notions and applications related to the subject;
- Damien Vergnaud, who gave a very simple but necessary introduction to public-key cryptography. He mentioned provable security and then moved to the actually employed encryption schemes and digital signatures based on the Discrete logarithm problem;
- Damien Stehlé, who introduced us to lattice-based cryptography. After providing the necessary background on euclidean lattices, he outlined the hard problems on which the security of lattice-based crypto systems relies, like the Closest Vector Problem and the Learning With Errors problem;
- Pierrick Gaudry, who deeply analysed the Discrete Logarithm Problem, pointing out the most recent discoveries on the subject;
- Léo Ducas, on lattice reductions and the choice of good bases to improve the performances of lattice based algorithms;

- Christophe Petit and Cole Martindale, on isogeny-based cryptography and applications of genus 2 and 3 curves respectively;
- Thijs Laarhoven, on lattice algorithms for the Shortest Vector Problem in lattice-based algorithms.

During my staying I met many other PhD students and created a good network with them. The winter school has represented a great opportunity to connect with other researchers and exchange ideas and knowledge.
Overall it has been a very satisfactory experience and I would have strongly suggested it to anyone who wanted a starting point for lattice-based cryptography and isogeny-based cryptography. For anyone interested, it is possible to download all the slides of the talk at
https://mathsofpkc.sciencesconf.org/resource/page/id/1