Post Quantum Cryptography Workshop
The University of Oxford, Mathematical Institute

18 - 22 March 2019

Wrya K. Kadir
University of Bergen

1 Motivation

Since 2017 NIST standardization process for post-quantum cryptography has been started and the second round announcements will be on April 1st. The workshop took place in March (18-22th), 2019 at the Mathematical Institute, University of Oxford. The event, that was by invitation only, was meant to bring together the top researchers in the field of Post-Quantum Cryptography for a week of fruitful discussions and exchange of ideas.

2 Presentations

Every morning we had two lectures given by specialists in each of the five main subareas of post-quantum cryptography. The overview and the techniques used in

- hash-based cryptography
- code-based cryptography
- lattice-based cryptography
- multivariate-based cryptography
- isogeny-based cryptography

were introduced during the lecture sessions. Moreover, Dustin Moody from NIST was invited to talk about the standardization process of post-quantum cryptography.

My favorite talk was given by Edoardo Persichetti about code-based cryptography. He started by some history about code-based cryptosystems and the reason why they have to be considered as post-quantum secure ciphers. The main ingredients to understand code-based ciphers were explained and then he continue by introducing the existing code-based schemes in Hamming metric. The main drawback of code-based schemes in Hamming metric is the very long key size. Then very recent schemes for instance RQC and Rollo were introduced. These

two schemes are very efficient in term of key size because they are based on rank-metric. Moreover, cryptanalysis of code-based schemes were discussed and the complexity of the attacks were shown.

3 Group Sessions

- After lectures the participants were divided in different group sessions to work and discuss on previously agreed problems. I joined rank-metric group session which I found it very useful. We had a very nice and friendly discussion with top researchers in this specific area including Tanja Lange, Philippe Gaborit, Thomas Johanson and Simona Samardjiska. They introduce new ideas that can be applied to attack rank-metric codes and also the reason why some ideas can not be applied to rank-metric based cryptosystems.

- RQC is submitted by Gaborit and his colleagues for NIST post-quantum standardization competition which has very nice properties and seems to be more concrete than other submissions based on rank-metric. At the moment my research focused on rank-metric codes and analysis the NIST submissions. I discussed with Gaborit and others, the properties of the used codes in this primitive and also the ideas to improve the performance of the system.

- In the rank metric group session the very recent attack based on ISD on rank metric by Gaborit which works better than Thomas Johanson's attack when $n > m$ was discussed. We tried to apply birthday paradox attack to improve the attack but we figured out this idea can not be applied due to the special properties of rank metric codes.

- Another idea by Tanja lange were discussed to improve the attack by reducing the search space. The idea is applicable if we combine it with quantum techniques.

- On Friday, the last day of the workshop, a member of our group Edoardo Persichetti presented the topics that discussed in the rank metric group to the workshop participants.

My trip was funded by COINS.