Spring School on Lattice-Based Cryptography

March (20-24th), 2017, Oxford (England)

Navid Ghaedi Bardeh

I got funding from COINS research school to attend Spring School on Lattice-Based Cryptography in Oxford, England, in March 2017. The venue of the spring school was in the Mathematical Institute, University of Oxford.

The spring school's aims were at bringing together PhD students, postdoc researchers and security experts from industry. It was a great opportunity to meet researchers from the common field of research. Well-known cryptographers were also lecturing, among them, Nigel Smart (University of Bristol) and Craig Gentry (IBM T.J.Watson Research Center).

The spring school topics varied, however, the main topics included:

- Mathematical Introduction to Lattices.
- Cryptanalysis, constructions and implementation of lattice-based cryptography
- Fully Homomorphic Encryption

Full program of the spring school, as well as presentation slides can be downloaded from the webpage of the program[1].

The spring school was opened by a speech on Mathematical Introduction to Lattices, by Richard Pinch. Next speech gave an overview of lattice-based cryptography. After lunch, another discussion was initiated; this time on Introduction to lattices, NTRU, Ring-LWE, and later Prof. Pinch continued his lecture on Mathematical Introduction to Lattices.

The second day started with an interesting topic on Ring-LWE: An Efficient PQC Public Key Encryption Scheme. After that, there was a session on Introduction to SageMath/Python.

The third day consecrated on cryptanalysis on lattice-based cryptography in three different lectures. In the last session, we had a lab that we implemented elementary cryptographic primitives based on lattices, a public-key encryption scheme in a single bit version, multi-bit version and ring version.

On the forth and last days, there was interesting lectures about Fully Homomorphic

[1] https://www.maths.ox.ac.uk/groups/cryptography/spring-school-lattice-based-cryptography

Encryption by Craig Gentry. His lectures during these two days covered a lot of interesting topics such as: Constructing HE, LWE-based encryption, Identity-based HE, HE form NTRU encryption and Key Homomorphism and Multikey FHE.

We had another lab in last session on forth day, which we implemented Gram-Schmidt orthogonalisation, LLL, BKZ, BKZ 2.0, Slide reduction and Self-Dual BKZ.

The spring school did not include topics very closely related to the field of study I am closely involved in, Symmetric Cryptography. However, as a new PhD student it was very useful to look at latticed-based cryptography and Fully Homomorphic Encryption.

Overall this school was a very nice event, which really interested me on especially Fully Homomorphic Encryption field. I got to meet new friends within cryptography, and I also got to discuss some important problems within my research with the top researchers in cryptography, which gave a lot of new ideas and approaches which help me a lot in my work.

I am deeply grateful for COINS supporting me to go to Spring School on Lattice-Based Cryptography.