Mathematical Methods for Cryptography

Andrea Tenti's report for COINS research school

September 4-8, 2017

Svolvær, Thon Hotel, Lofoten, Norway

The conference Mathematical Methods for Cryptography (MMC) was held the first week of September in Svolvær for celebrating Tor Helleseth's seventieth birthday. The Lofoten Islands have been the perfect scenario to host many leading characters in the field of cryptography and information security as well as young researchers.

The complete program description together with the abstract of all the talks can be found at http://people.uib.no/chunlei.li/workshops/lofoten/index.html. Moreover there will be a special issue of the Journal "Cryptography and Communications" containing the papers of the most relevant talks.

The talks touched many topics such as:

- Coding theory,
- Cryptographic primitives,
- Algebraic tools for cryptography,
- New results in symmetric cryptanalysis,
- Theory of boolean functions.

At the moment my research project involves cryptanalysis of elliptic curves DLP and currently I am trying to use mathematical tools that were developed in the cryptanalysis of symmetric ciphers with some promising results. The conference has been a milestone for my research thanks to the

ideas and methods suggested during some of the talks. The most influential in this sense were:

- "Representing integer multiplication using binary decision diagrams" by Håvard Raddum (joint work with Srimathi Varadharajan),
- "Current trends in linear cryptanalysis" by Kaisa Nyberg,
- "Re-Linearization and elimination of variables in boolean equation systems" by Bjørn Greve (joint work with Håvard Raddum, Gunnar Fløystad and Øyvind Ytrehus),
- "Recovering short generators of principal fractional ideals in cyclotomic fields of conductor pq" by Patrick Holzer (joint work with "Thomas Wunderer and Johannes Buchmann),
- "An algebraic approach to the design of block ciphers" by José Manuel Valerença (Joint work with Óscar Pereira).

In addition, other talks in the conference stroke my imagination and helped me to gain a wider comprehension of the tools and the research interests involved in cryptography. Among them I mention the following:

- "A perspective on cryptocurrencies" by Bart Preneel,
- "Hardware design for supersingular isogeny Diffie-Hellman key exchange" by Lejla Batina (joint work with Pedro Maat Masolino and Joost Renes),
- "Characterizations of differentially uniform functions by the Walsh transform and related cyclic difference set-like combinatorial structures" by Claude Carlet,
- "Column-parity mixing layers" by Joan Daemen,
- "Secure and robust data services in Cloud and Fog" by Chunming Rong

The experience has been, overall, of key relevance for my growth as a researcher and I am grateful to COINS for having allowed my presence there through financial support.