Report from CrossFyre 2018

Martha Norberg Hovd

CrossFyre is an annual workshop for young female researchers in cryptography, information security and other related fields, held at a different university with a strong research group every year. Previous hosts include Darmstadt, Germany and Eindhoven, Netherlands. The host university this year was University of Surrey in England, and the workshop lasted for two days, with 13 talks by participants, six talks by invited speakers and a panel discussion on appropriate ways of encouraging women into male dominated fields, and mathematics, information security and cryptography in particular.

The talks given by the participants were on a large variety of subjects, reflecting the diversity of the fields of study for the various researchers. The topics ranged from the practical security of a feature called 'message franking' by Facebook to highly mathematical and theoretical proofs of security. Among the talks that stood out was a presentation given by Laura Shipp on her research on the security in apps allowing women to track their menstrual cycle. These apps collect highly sensitive information, such as whether or not the user is pregnant, and yet Shipp demonstrated how the security of the apps are all but lacking. The talk given by Fatma Al Moqbali on web-based solutions for password recovery was also very interesting, as she showed how practically all currently used methods are insecure, in the sense that they may leak some, or all, information about the user, previous passwords and may even help an adversary find passwords used on different platforms. This final point is due to the fact that many sites use the same questions (e.g., 'what is your favourite animal?') a user should answer in the event he or she wishes to recover a lost password, and if an adversary finds the answer to one of these questions, she may use this answer for other log-in platforms.

I was one of the participants who held a presentation, based on the article *A Successful Subfield Lattice Attack on a Fully Homomorphic Encryption Scheme,* which I was due to present the following week at the Norwegian Information Security Conference in Svalbard. Although experience giving presentations is always valuable, especially to an audience in your own field of research, the timing of the workshop gave me the opportunity to have a 'test-run' of the conference presentation, which was very valuable. Furthermore, the setting was rather informal, which I believe resulted in more, and possibly different, questions being asked, compared to a regular conference.

Amongst the invited speakers were women with long and successful careers in both the industry and academia. One was a top cryptographic researcher at the National Cyber Security Centre (NCSC); another had worked for decades in Hewlett Packard Laboratories as a principal research scientist and is now a professor at the University of Surrey. Although the talks these speakers gave were interesting, the one that was most memorable was the presentation given by Chris Bruzska, who spoke about his transition from female to male, how he had approached this like a mathematician, and the reflections he had made about gender as a whole because of this transition.

The presentation by Bruzska and the panel discussion were the only clearly gendered items on the agenda, and I found both very rewarding. It was interesting to hear other women's thoughts about such things as the pay gap and gendered quotas during the panel discussions, as well as suggestions on how girls may be recruited into the STEM fields. We discussed for example if "girl camps" and similar activities may help achieve this, or if they may actually be counterproductive, as separating the genders at an early age may support already existing beliefs that girls somehow need "more help" or special attention when it comes to mathematical and technical subjects. As was the case with the presentations in general, the panel discussion was rather informal, resulting in an actual discussion, as opposed to a couple of participants stating their views and everyone else merely listening in.

In addition to the talks and discussions, the networking was a key factor of the workshop, and a quite enjoyable factor as well. It is nice to share two days with people who not only shares your interest in your research area, but also is able to relate to an experience of being female in an area so vastly populated by men, and with interesting reflections related to this to boot. As a fairly new PhD, I have realized that getting to know people is quite important, not only because it increases the probability of finding a familiar face at a conference sometime in the future, but also with regards to getting a foot in the door with respect to research stays and the like.

Overall, the workshop was an interesting and rewarding experience, not only because of the opportunity to practice giving a presentation I was due to hold at a later conference. The workshop also demonstrated the great variety of research being performed, and furthermore by women. It is easy to forget sometimes that there are more women in cryptography and information security than the handful I already know, and CrossFyre is a great reminder of the fact that women are doing both interesting and important work in these fields as well.