Reflection report from Arctic Crypt 2016

Martin Strand (martin.strand@math.ntnu.no), August 2016

Arctic Crypt was arranged for the first time in July 2016, and gathered approximately 80 participants and 20 accompanying persons in Longyearbyen, Svalbard. Despite being a first, the exotic location attracted several top names from the crypto community, which led to a very interesting conference.

The program had a nice combination of invited talks and submitted works, meaning that it felt more coherent than some small-but-general conferences sometimes do.

For my part, the highlights of the week was

- Gizem Çetin, Yarkın Doröz, Berk Sunar and William Martin: Arithmetic Using Word-wise Homomorphic Encryption
- Adi Shamir: How Can Drunk Cryptographers Locate Polar Bears (midnight talk)
- Greg Rose: KISS: A Bit Too Simple
- Dan Bernstein: NTRU Prime
- The excursion to Pyramiden

The crypto community excels in making new members feel welcome. I always find it easy to engage in discussions with anyone, no matter their past merits. So was also the case at this conference, and while the program itself was strong, the coffee brakes are just as important.

Unfortunately, I had to leave the conference before it was over due to other duties. One should therefore look up the report from Herman Galteland to learn more about the last part of the conference.

Arithmetic with FHE, locating polar bears, ...

Fully homomorphic encryption is still a hot topic after its 2009 discovery. However, the number of new schemes being proposed seems to have gone down, and more people are focusing the effort around investigating the properties of the ideas and schemes that have already been published. One particular challenge has been to perform divisions in addition to adding, subtracting and multiplying. The main reason for this is that a division usually

requires computing an inverse, which again can demand a high number of (expensive) multiplications. The authors that presented at Svalbard used a floating point representation of the numbers, and then used numerical methods such as Newton's method homomorphically on the data to find the result of a division. The advantage of this approach is that one can limit oneself to reasonably cheap operations, and they also described how one can compute the square root of an encrypted value. Together with some other recently published work, this can improve the applicability of FHE.

Ron Rivest and Adi Shamir delivered one talk each during the midnight session (11 pm–1 am), and the sun also gave the participants a brief audience through the window. Shamir had gotten hold a rifle (minus a vital part, that must be said), and used drunk cryptographers with a very limited memory and polar bears with converging tracks as an allegory. The main point was on how one could use nested Pollard-rho techniques to find a needle in a very large haystack.

Greg Rose demonstrated how the KISS random number generator is completely flawed, and should be avoided at all costs.

Dan Bernstein has done considerable work on post quantum crypto, and was forcefully driving home an important point about newly proposed hardness problems and concrete parameters for schemes: Many could use more analysis before being considered safe to use.

One day was dedicated to a boat trip to a deserted Russian settlement, Pyramiden (The Pyramid). At its peak, the town had over 1000 inhabitants, but its infrastructure matches that of a much larger place. Facilities included a concert hall, ballet room, gymnastics, indoor swimming pool, a large cantina with free food around the clock, pleasant architecture and Ukrainian soil in order to have greener lawns. The reason, we were told, was that Pyramiden was one of very few Sovjet settlements available to the west.

All COINS students had a group picture taken during the boat ride, in front a large glacier, *Nordenskiöldbreen*. The weather, however, did not permit us wearing any gear visibly – so we would have to make due by holding a sweater. The picture will be submitted by another member of the group.