Arctic Crypt 2016

Herman Galteland

Being the northernmost crypto workshop ever held, the Arctic Crypt 2016 conference was in Longyearbyen, Svalbard at 78° north. Despite having a limited capacity of facilities, the workshop attracted a wide variety of prominent invited and submitted presentations (due to its exotic location). The program co-chairs for Arctic Crypt 2016 was Tor Helleseth (University of Bergen) and Bart Preneel (University of Leuven), the general chair was Øyvind Ytrehus (University of Bergen and Simula).

Including to its academic contents, the conference also included several social activities; including lunches, dinner, and a one day excursion where the participants went on a boat trip to look at the wildlife, the unique scenery, and an abandoned coalminers settlement.

Invited Presentations

The workshop consisted of both invited and submitted presentations, with a wide variations of topics. The following is a short summary of some of the invited talks

- ***Codes and stream ciphers:*** Some new results on the QC-MDPC (Quasi-Cyclic Moderate Density Parity Check Code) cryptosystem, which is a code based encryption scheme, like the McEliece Cryptosystem, that use a p-alphabet instead of a binary alphabet.

- ***Authenticated encryption:*** A presentation of the keyed sponge and how it was used in Keccak.

- ***NTRU prime:*** Related to post-quantum crypto and how we should not trust provable security. The DL problem and factorization can be broken given access to quantum computers, hence it is not secure to blindly base security on the hardness of these problems.

- ***Public key cryptography:*** Two presentations, the first look at the probable security of DSA and ECDSA signatures, and the second asked when and how we should convert to a new standard using crypto that is secure in a post-quantum world.

- ***Block ciphers:*** An update on the block ciphers *LowMC* and *MiMC*. They are designed to be efficient for FHE and/or MPC, and try to use as much linear operations as possible while still being secure.

- ***Midnight lectures:*** Most notably was the two midnight lectures. First was "symmetric encryption based on keyrings and error correction" by Rivest, where he discussed how to use a set of words as keys instead of a random string. Second was "how can drunk cryptographers locate polar bears" by Shamir, or in other words "a low memory needle in a haystack problem", where he presented a variation of the Pollard-Rho algorithm. Note that during the summer it is midnight sun at Svalbard.

Submitted Presentations

The following list is a short list of some of the submitted talks.

- KISS is a simple pseudo random number generator, do not use it if you value security.

- An analysis of a homomorphic encryption scheme, verifying the validity and giving a presentation of three attacks.

- Arithmetics using word-wise ($\mathbb{Z}_q$) homomorphic encryption, instead of bit-level ($\mathbb{Z}_2$).

- More efficient implementations of multiplication, e.g., karatsuba, however, the overhead might increase.

- Quantum crypto; assuming quantum computers exists, but communication is still sent as normal signals.

- Security analysis of BLS and BGLS signatures in a multi-user setting. The multi-user setting covers the setting where the sender encrypts, under different keys, plaintexts that is related to one another (such as in a signature scheme).

- Timing attack on OpenSSL constant time RSA nicknamed CacheBleed.