Arctic Crypt 2016

Britta Hale

True to title, Arctic Crypt 2016 took place in Longyearbyen, on the Svalbard archipelago. With its unique location, and consequential limit on transport and accommodation resources, attendance at Arctic Crypt was self-bounded to under 75 participants. There were many interesting talks throughout the conference, including on the current state and future of post-quantum crypto, and even invited talks not summarized here. However, this report focuses on a few presentation examples to achieve both conciseness and depth in summary, providing a taste of the discussion which occurred at 78^o north.

Thomas Johansson: Some new results on QC-MDPC Thomas Johansson opened with the first talk of ArticCrypt with motivation for post-quantum cryptography and the McEliece PKC system variant QC-MDPC. After briefly commenting on the four quantum system research areas (lattice-based, code-based, hash-based, and multivariate cryptography), the talk focused in on the code-based McEliece system. Despite McEliece cryptosystem enjoying a long existence, having been proposed in 1978, large key sizes have been a daunting drawback to actual use. However, the 2013 Quasi-Cyclic Moderate-Density Parity Check (QC-MDPC) variant has allowed key sizes to be reduced to 4801-bit while achieving 80-bit security. MDPC code is a linear code using a sparse parity-check matrix with row weights in the scale of $O(\sqrt{n \log n})$. In order to protect against various attacks, CCA security is achieved via *CCA conversion*, in which the choice of error vector $\mathbf{e}$ is done at random. Current improvement work in modifying QC-MDPC is on-going, with an overall goal of optimization.

Sonia Bogos, John Gaspoz and Serge Vaudenay: Analysis of a Homomorphic Encryption Scheme In this talk, presented by John Gaspoz, the authors analyzed the security of a Somewhat HE scheme by Zhou and Wornell. The particular scheme which was analyzed is based on linear algebra and is deterministic, with security based on LWE (Learning With Errors) and the SIS (Short Integer Solution) problem. Three successful attacks were presented against the protocol: an attack on broadcast encryption, chosen ciphertext attack, and a chosen plaintext attack. The attacks were successful enough to provide an attacker with the actual plaintext.

Gizem Cetin, Yarkin Dorz, Berk Sunar and William Martin: Arithmetic Using Word-wise Homomorphic Encryption In a very nice presentation by William Martin, HE was explored further, with discussion focusing on word-level encryption instead of bit-level, the latter of which yields larger ciphertexts. The talk branched into threshold functions (control over the threshold at which the function outputs y) and approximation via the Fourier series for the square wave, when handling words with decimal representation. Martin concluded with implementation details and a comparison of circuit-depth for binary and word-wise operations, demonstrating lower circuit-depth in the latter case. However, word-wise operations still showed efficiency issues under division, equality checking, and comparison, leaving room for future improvements.

Taking advantage of the midnight sun in Svalbard, Arctic Crypt hosted its very own *Midnight Lectures*, with guest lectures by Ron Rivest (via Skype) and Adi Shamir:

Ronald R. Rivest: Symmetric Encryption via Keyrings and ECC Rivest, via Skype, spoke on issues related to keyrings and simplifying key updates. In particular, he focused on resilience, where encryption between parties should be possible even if keyrings are slightly out of sync, and translating the distance metric for set size to a Hamming distance between keyring words for error correction.

Adi Shamir: How Can Drunk Cryptographers Find Polar Bears In a lively midnight-01:00 lecture, Shamir undertook the needle-in-a-haystack problem of finding a biased output y_0 in a nearly uniform probability distribution. The simplest memoryless algorithms would loop over all possible events or use the generator to suggest the next possible output. However, Shamir argued for a model based on pseudo-randomness, where the same input into the distribution generator should give the same output each time, and using a deterministic generation based on an iterated random walk through the values allows for the same point to be encountered multiple times. Using a nested-Rho algorithm technique (up to 4-time nesting) allowed for reduced time complexity over previous algorithms.