Travel Report

Åvald Åslaugson Sommervoll

1 NordSec introduction

The 23rd Nordic Conference on Secure IT Systems is abbreviated to NordSec 2018. This year, the conference took place from the 28th of November to the 30th of November at the Department of Informatics at University of Oslo in Oslo, Norway. The NordSec is an annual conference which has been ongoing since 1996 and covers a wide range of IT security topics, with the aim of bringing together computer security researchers in Northern Europe and beyond, and encouraging interaction between academia and industry. In addition to being a venue for academic publishing, NordSec is an important meeting place for university faculty, students, and industry researchers and experts from the region. The proceedings consist of peer-reviewed articles and are published in the Springer Lecture Notes in Computer Science series.

2 Revisiting Deniability in Quantum Key Exchange

PhD candidate Arash Atashpendar begins by describing the original motivations behind revisiting deniablity in quantum key exchange. Namely to overcome classical no-go results using quantum information and tackling coercion-resistance in secure e-voting. In dealing with coercion-resistant e-voting Atashpendar et al. strive for deniability[1], which is also essential in off-the-record messaging, anonymous reporting and whistle blowing.

While deniability has been explored, it remains largely unexplored by the quantum crypto community, with only single prior paper by Donald Beaver. In this paper, he argued that quantum key exchange not necessarily is deniable due to an eavesdropper attack which limits key equivocation. However, this was formulated before deniability was formalized for AKE (authentication key agreement). So the presenter, Arash Atashpendar, hints that they solved this issue.

The speaker then briefly covered quantum computation, the superposition principle, the measurement principle, unitary evolution and qubits. Before covering quantum key exchange:

[1] Deniability refers tot the ability to deny a message or action.

1. In this exchange, Alice generates two random bit strings and encodes one of them into a quantum based on the other bit string.

2. Bob then receives a series of quantum states from Alice. Bob also draws a random bit string and measures the quantum states according to this random string.

3. Alice and Bob compare basis-es, and keep the bits measured by the same basis.

4. Alice and Bob estimate their error rate, if it exceeds a threshold they abort (and start over)

5. Error correlation is then applied to give Bob and Alice keys of equal length. (An eavesdropper may have partial knowledge of these keys)

6. Apply a secret distillation to convert the error corrected keys into shorter, but secure keys.

Then using such a key exchange technique, coercer-deniable quantum key exchange was defined, and a template for such a key exchange was presented. A technique which utilizes the entanglement distillation and teleportation properties of a quantum computer. The speaker ended concluding that there is much room for more work in deniability using quantum cryptography, and listing future work.

3 Poster session

Norwegian cyber range presented by PhD Muhammad Mudassar Yamin covered an exercise where two teams (red and blue team) compete as attackers and defenderes in a virtual and physical environment developed by a white team. This provides a better training ground than autonomous systems. **User Perception Analysis for Showing Personal Data Access as privacy implication factor** presented by Nurul Momen and Sven Bock covered an alternative app store interface with privacy indicators, which indicate how invasive the listed application is. **Chunk Encryption and Redundancy Matrix Representation for Reversible Data Hiding in Encrypted Images** presented by Chi-Man Pun hid information in encrypted images so that for example doctors can see patient information without decrypting the images.