A report on my attendance in the student seminar and NISK conference in Longyearbyen

My travel to Svalbard was so amazing and brought me precious memories and experiences. I enjoyed both academic and social events during the Norwegian ICT conference (NIKT). On the first day, I participated in the COINS workshop. It consisted of several presentations where 3 PhDs shared their experiences and lessons from doing their PhD. They mainly emphasized on common notes: having a balance between work and life, finding interesting topics, setting clear times and goals for completion of the work, having regular and effective meetings with the supervisors, working and communication with people from your field and educating yourself. The most important message that we received was: "Do your best and NOT give up easily!"

In addition to these, we listened to some interesting technical talks from COINS members. A talk by Adam Szekeres targeted the limited and promising approaches for human decision making in the field of IoT security. A presentation by Ali Khodabakhsh, was about fake face recognition using biometrics approach. The main contribution was developing classification techniques based on machine learning models which use human face characteristics and calculations for correct recognition. Mazaher Kianpour talked about cyber risk quantification techniques. He introduced behavioural economics to find potential reasons for security risks and suggested using Network Game theory and NetLego simulation system as proper solutions. After a presentation by Shukun Tokas about optimization of General Data Protection Regulations (GDPR) framework using language-based mechanism, Berglind had a presentation about life after PhD. She talked about her tireless endeavour to find a job after she did her PhD. In final talk, Bikash Agrawd explained about the requirements of start-up companies, and his own experience on establishing an ICT-based start-up company in Norway known as Boost.AI. The workshop finished by voting for two COINS student representatives. At the end of the day, we went to an interesting and informative sightseeing tur by bus around the city.

The opening day of conference (Wednesday, September 19th) started by a UDIT keynote by Barbara Wasson on learning analytics (LA) and its role in education. She defined learning analytics as the measurement, collection, analysis and reporting of data about learning and other contexts for the purpose of understanding and optimizing learning and the environments in which IT occurs. Then she introduced some common architectures in this field where different processes mentioned above interact together. She continued with mentioning different types of historical and new data in education field and role of LA on that. The talk followed by introducing the main themes within this filed such as LA for educators and institutions. Then the gaps in the research were addressed such as application of LA in K-12 education, research on assessment and feedback and research on learning centric analytics versus learner-centric analysis. She finalized her talk with talking about their completed and current projects and LA applications in Norway like Multi Smart Øvning at schools, CANVAS without analytics from higher school and CONEXUS from Edtech.

Martha Norberg presented a successful subfield Lattice Attack on a fully homomorphic encryption (FHE) scheme. According to her analysis, in the FHE scheme, both multiplication and addition are respected homomorphically, leading to a reduction in Degree 'd' of a ciphertext and the absolute value of noise. However, it imposes the additional operations such as KeySwitch and ModSwitch. These operations introduce bounds on the parameter 'q', where satisfying these bounds, makes the FHE scheme susceptible to the subfield Lattice Attack.
Another talk by Slobodan Petrovic was about improving the generalized correlation attack against stream ciphers by using bit parallelism. First, he clarified the possibility of correlation

attack on a non-linear combiner where output sequences are combined in a non-linear Boolean function such as Linear Feedback Shift Registers (LFSRs). Then, in more advance level, he claimed that still, a non-linear combiner with irregular clocking is susceptible to break by generalized correlation attack which employs constrained edit distance computation. In their study, they proposed constrained approximate search and bit-parallel implementation to address the limitations of generalized correlation attack in terms of quadratic time and space complexities for the distance computations.

Tjerand presented the results of their experiments on the web security. In this research, they scanned the top 500 most visited sites from nine countries of interest in addition to documenting the HTTPS usage, the encryption algorithms and certificate information. Based on their analysis, the United States, Norway and Canada have the highest percentages of top sites using HTTPS, while China and Iran have the lowest fractions. RSA and SHA256 are the most common signing algorithm used versus SHA1 and RSA with fewest usage. Major browsers in China and Iran were identified as in-secure since they work under invalid and not updated certificates. He concluded that the users from countries with security issues are more susceptible to eavesdropping or corrupting data while sending data over the internet. He also mentioned the policy makers and stakeholders can use this information to set more protective policies on the websites (using HTTPS and HSTS) and finally private sector actors are more involved in web security initiatives such as Let's Encrypt certificate authority.

In an interesting presentation by Patric Bours, a scheme for fake chatroom profile detection was introduced. This work which mainly belongs to cyber safety projects, aimed at protecting children online from sexual predators or cyber bullying. The main limitation in these kinds of studies is limited access to real data due to privacy issues. Therefore, they conducted the experiments on the data sources where the children were fake, and the conversations were full. They used biometric analysis to find out unique typing rhythm and Stylometry to find unique writing styles. In the text analysis, word choice was considered as an indicator for identifying gender, age and emotional state. In their future work, they plan to work on author profiling, grooming detection perverted-justice data and grooming detection on real data.

Per Meland talked about combining threat models with security economics to improve cyber risk quantifications. In this model, the attack and defence, agent profiling and graphical notations from threat models can be combined with incentives, externalities, cost data and utility from security economics. Area of concern can be exposure of new technology and traditional safety predictions based on historical data. Little help from hindsight, poor security investments and stochastic behaviour of adversaries are introduced as the main problems. He concluded that in a generic risk model, different factors should be considered such as domain and Geo data, profile and vulnerability data, threat taxonomy, incident data and specifically attacker cost.

In the final talk of the day by Roman Vitenberg, seven common blockchain myths were introduced. He explained how each of these myths cannot be partly or completely true. 1-blockchain is similar to another storage technology like distributed database. It was rejected because the trust model between blockchain and distributed DB is different. The nodes in blockchain do not send data indiscriminately to other nodes.2: Blockchain has a universally agreed definition. But this cannot be completely true since there are a lot of definitions and ambiguity there.3-Block chain and Bitcoin are interchange in terms of terminology. Whereas Bitcoin is a specific system versus ambiguous blockchain that can be structured used in Bitcoin or a separate concept. The fourth and fifth claims about Block chain that were rejected included

all blockchain technologies use mining, deploy a P2P network and consume lots of energy. Even the claims about private blockchain are not true when it is said that private Blockchain are necessarily lacking transparency or belong to the private sector.

On Thursday, the first speaker was Lars Knoll, the CTO of the Qt company. He talked about his experiences gained through 20 years of Qt. Qt was introduced as probably the most comprehensive C++ framework available today which is being used for both application development and device creation. One example of QT application is in air traffic control systems to monitor air traffic. Qt started in 1997 where KDE project built a Linux desktop using Qt. Today Qt has more than 285 professionals in 12 countries, provides services to more than 70 industries and 5000 customers. The new technologies that they seek improvements on are Artificial Intelligence, Analytics, cloud computing and IoT.

The second presentation by Tommy Thorsen was about accessing face image quality with LSTMs. In this work, they wanted to ensure good performance of face recognition authentication systems. To solve the problem, they proposed using machine learning algorithm known as CNN and LSTM. A variant of LSTM capable of working with multidimensional data known as 4-way LSTM, and a variant of CNN called AlexNet model were combined to produce the final result. They conducted the experiments on a Samsung S7 database and measured the performance of their proposed model using Error Reject Curves (ERC). In comparison with other techniques such as AlexNet, LSTM and commercial solution, their quality assessment algorithm with simpler implementation performed well. However, some drawbacks of this approach is that the resulting framework file is large, running estimation function is slow and training the network takes a long time. For future work, they recommended scaling down the size and complexity of the network and using some variants of LSTMs that can be parallelized.

Another talk was about designing a verification system as a baseline evaluation of smartphone-based finger photo. In this research, they developed an iOS app to capture the image or videos of fingers. They introduced two methodologies for feature extraction: Local Binary Pattern Features (LBF) and Binarized Statistical Image Features (BSIF). According to their experiments and results, the performance of commercial systems is better than all baseline non-commercial systems, since the mentioned feature extraction methods were not successful enough. However, they concluded that employing advance pre-processing methods would lead to improvement in feature extraction and model performance.

In the last presentation of the day, Marta Gomez introduced a fingerprint attack detection (PAD) method based on short infrared imaging and spectral signatures. She talked about the security issues of biometric systems which allow a reliable and automatic person authentication. She divided these security attacks into two parts: Presentation attack which may take place before feeding the sensor with a biometric characteristic and software attacks. The second attack may occur in different phases after sensing, but the first attack is highly dangerous because it is easy to implement, without knowledge of the inner modules and easy to carry out like door or smart phone unlocking. Their solution is a new fingerprint PAD method which relies on the analysis of skin reflectance properties for the SWIR band. The performance was analysed with the ISO/IEC IS 30107-3 on PAD for a dataset including 12 different PAI species. A low attack presentation classification error rate (APCER) was reported in their preliminary results, but the model could not detect playdoh fingers which are visually similar to the bona fides. Using CNN and larger datasets are considered in their future work.
Finally, we spent a unique evening in Camp Barentz, where traditional Norwegian reindeer dish was served, and we listened to interesting stories from Spitsbergen and about polar bears.