Quantum Key Distribution

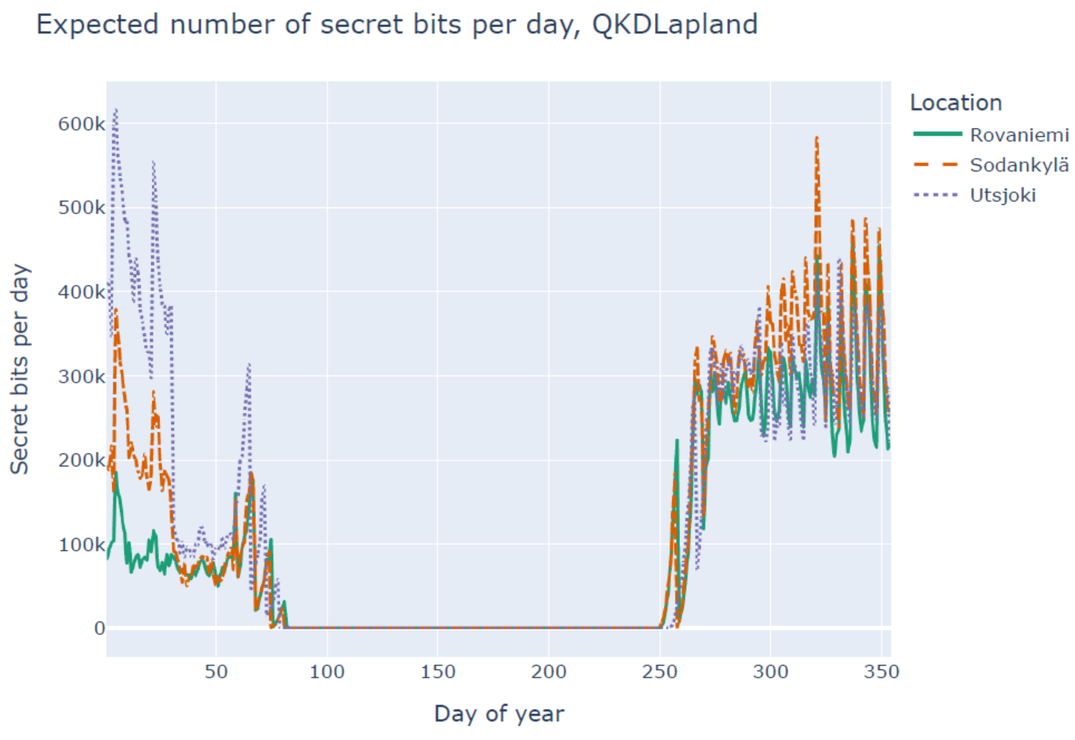
Authors: Sara Nikula

Satellite-Based Quantum Key Distribution in the Arctic: A Case Study of Finnish Lapland

In this paper, a QKD link was simulated with MATLAB for two satellite trajectories and three optical ground stations located in Finnish Lapland. The results show that although the polar night provides highly favorable conditions for satellite-based QKD, cloud cover and persistent background illumination during the brighter half of the year impose severe constraints, necessitating long-time storage of the generated key material.

Figure 1. Simulated ground station locations in Finnish Lapland. Base map: OpenStreetMap [26]; annotations and labels added by the authors.

On average, the simulated satellite connection could generate 85927 secret bits per day between Rovaniemi and Utsjoki stations. Depending on the month, cloud cover blocked the key distribution with a probability of 41—76 %. Other considered weather conditions included fog, rain, sleet, and snow, based on weather data from FMI.

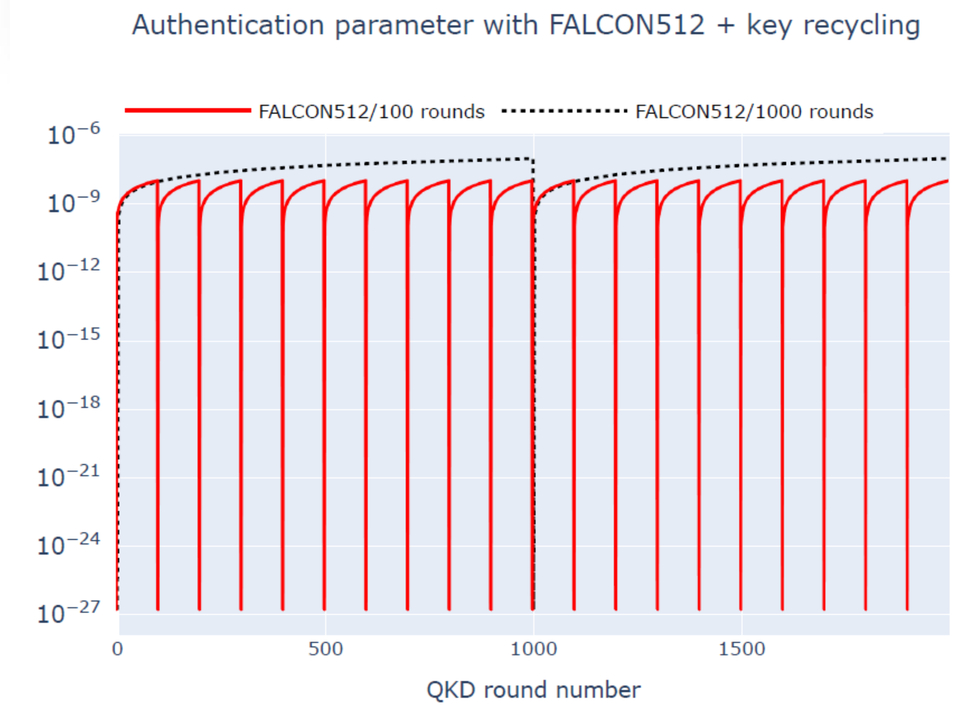


Paper available online: Nikula et al 2026 *J. Phys. Commun.* https://doi.org/10.1088/2399-6528/ae57f7

Combining digital signatures and key recycling in QKD authentication: a performance and security analysis

This paper investigates the feasibility of combining digital signatures with key recycling in QKD. The results indicate that such an approach is viable; however, the security parameters employed in QKD and PQC are highly incompatible, leading to significant fluctuations in the authentication-related security parameter.

This paper was presented at the International Conference on Information Technology and Communications Security (SECITC) 2025, Bucharest, Romania, and will be published in LNCS series.



If the first QKD session is authenticated with a digital signature with security parameter 2^-89, and a portion of the QKD-generated key is then saved for authenticating the next session, the authentication parameter will increase sharply if a conventional QKD security parameter is used.

Conclusion

- **Satellite-based QKD is feasible in Finland, but:**
  - **Finland typically has high probabilities of cloud cover, which blocks the QKD signal**
  - **Continuous background light during the summer period in polar regions poses challenges for QKD devices, which are sensitive to light**
- **Post-quantum digital signatures can be used together with authentication key recycling in QKD, but:**
  - **QKD security parameters must be reassessed**

Contact: Sara Nikula, Research Scientist
Tel. +358505344268, sara.nikula@vtt.fi