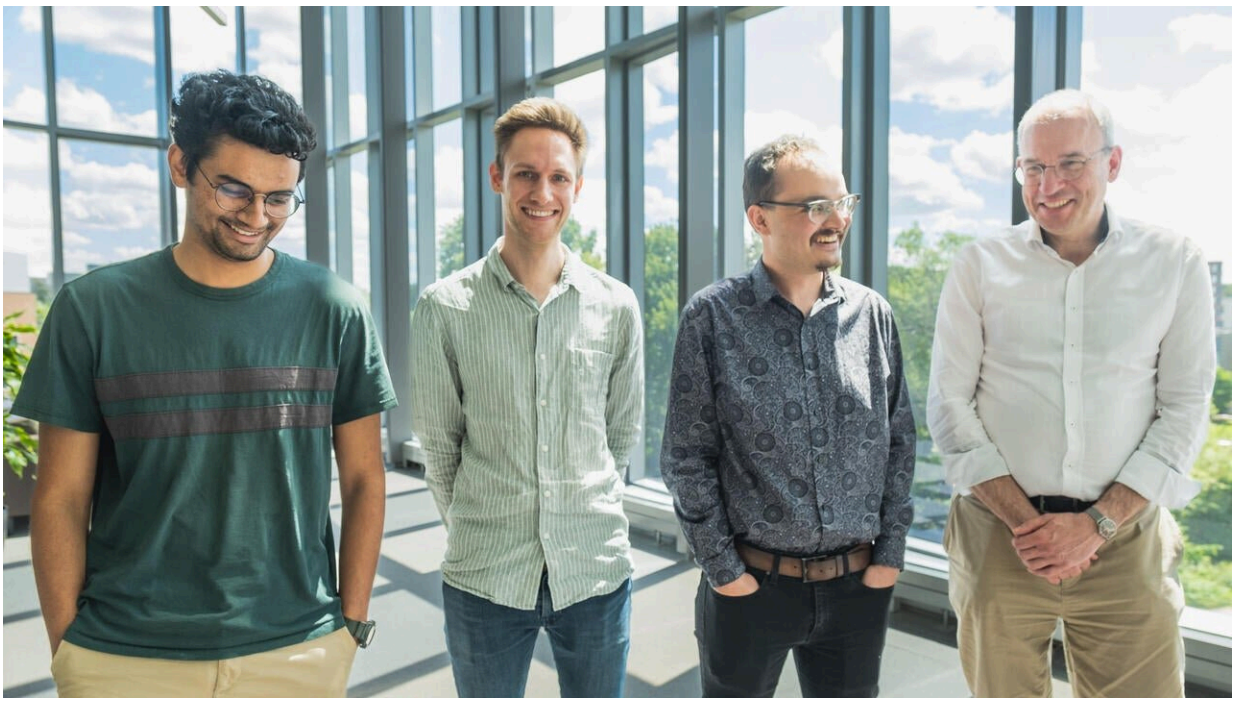
New open-source software for quantum cryptography is greater than the sum of its parts

July 3 2024, by Elizabeth Kleisath



From left to right: PhD students, Devashish Tupkary and Lars Kamin, John Burniston, Waterloo researcher, and Dr. Norbert Lütkenhaus, executive director of the Institute for Quantum Computing. Credit: University of Waterloo

Accurate models of real-world scenarios are important for bringing theoretical and experimental research together in meaningful ways.

Creating these realistic computer models, however, is a very large undertaking. Significant amounts of data, code, and expertise across a wide range of intricate areas are needed to create useful and comprehensive software.

Dr. Norbert Lütkenhaus, executive director of the Institute for Quantum Computing (IQC) and a professor in the University of Waterloo's Department of Physics and Astronomy, alongside his research group, have spent the last several years developing accurate software models for research in quantum key distribution (QKD).

QKD is a process for cryptography that harnesses fundamental principles of quantum mechanics to exchange secret keys, which can then be used to ensure secure communication.

Lütkenhaus and his research group recently released a modular, open-source software package on GitHub, which allows users to model realistic QKD protocols and calculate the generation rate for secure quantum keys using user-submitted variables for real-world scenarios.

"Modeling and analyzing QKD setups require many different skills to come together. Our software framework allows experts in various areas like optimization theory, optical modeling and security analysis to bring their knowledge together," Lütkenhaus says. "The open-source approach is designed to foster an interdisciplinary community from which all researchers will benefit."

While creating their realistic models and protocols, the team considered a wide range of problems that present different challenges in the coding process, and then split the problem from one single, monumental coding challenge into smaller pieces and modules. By doing this, the team was able to lean on the varying expertise of its members and bring in collaborators in specialized areas.

"QKD models with realistic assumptions require a lot of information and knowledge across a huge number of domains. Especially if you want to interface them with experimental data or realistic models which we're not necessarily the experts on," says John Burniston, the lead developer of this software package and a research associate at IQC.

"Our software breaks down this monumental task into smaller chunks, so it's gone from the task of 'I needed to learn everything' to 'let me solve this part and incorporate it with others,' which is less daunting."

In addition to incorporating the necessary range of expertise during the software development, the modular nature is also a benefit to teaching and training new researchers and students. New undergraduate researchers can be directed to a single module, where they focus on learning and optimizing just one aspect or variable within the overall QKD model.

Since their changes can then be incorporated into the overall software package, the students are able to see how the changes to their small section can impact the overall scope of the problem and outcome of the QKD key rates.

The new software package is a complete rewrite of a previous version released in 2021, which has now been optimized to enhance the user experience. With more smaller module chunks, and more internal checks and balances for validation, the software can identify to users if an inputted value is realistic and correct or if it is likely to give a meaningless output. Overall, these updates create software that is easier for someone to learn and incorporate into their research.

Currently, Lütkenhaus' group is working with several collaborators to develop new modules for the software package and apply their QKD software modeling in experimental research labs.

Lütkenhaus' group has partnered with different teams from Waterloo: Dr. Henry Wolkowicz and his group from the Department of Combinatorics and Optimization, on numerical convex optimization; and IQC's Dr. Thomas Jennewein and his group, to model key rates for satellite QKD applications.

They also have partners from other institutions working on a variety of realistic modeling problems. Using their software models, they have already found ways to significantly improve experimental key rates with their collaborators.

By publishing this software package as open source, the researchers hope to encourage the QKD scientific community to collaborate and grow. To facilitate this collaboration, they are planning an upcoming training session for researchers from around the world.

Details will be announced on the project website once finalized. Additionally, the software package also aims to decrease the gap and provide connections between theory and mathematical proofs with experimental data and building devices.

"It's fun to blend together work on software development with cutting edge research," Burniston says. "We can give this new tool to everyone, help out the greater community and really push the research forward."

Provided by University of Waterloo

Citation: New open-source software for quantum cryptography is greater than the sum of its parts (2024, July 3) retrieved 3 July 2024 from https://techxplore.com/news/2024-07-source-software-quantum-cryptography-greater.html