“R10”, Open Source AIT QKD software for QKD post processing

Oliver Maurhart, Christoph Pacher,
Cristina Tamas, Andreas Poppe and Momtchil Peev

AIT Austrian Institute of Technology, Donau-City-Strasse 1, 1220 Vienna, Austria

This presentation discusses the recent modifications and extensions of the “R10” of the AIT QKD post processing Open Source Software. This software is a great overhaul of the work derived from the results on trusted repeater QKD networks, obtained in the SECOQC project. It provides an concise and easy to use array of building blocks to integrate arbitrary sifting, reconciliation, privacy amplification and other post processing tasks and allows in principle a full-scale QKD network integration.

The latter objective relies heavily on the Quantum Point-to-Point Protocol (Q3P) that accompanies the QKD post processing stack and realizes the trusted node paradigm, which allows Information Theoretically Secure (ITS) network-wide key distribution and correspondingly secure peer to peer communication for classical applications.

At the heart of the QKD design lies the “QKD Module” realized as a UNIX process, which reads in key material and performs various tasks on this data stream, ranging from simple BB84 protocol sifting, to LDPC algorithms and beyond. These modules are designed for serial interconnection with one QKD module providing input for the next. The connectivity between the modules is based on Zero Message Queues (0MQ), a thin Inter Process Communication (IPC) layer, which makes QKD modules resilient and fast at the same time. As all QKD modules share the same input/output interface provided by the AIT QKD library written in C++11, integration of novel protocols or algorithms is straight forward.

Among the new modules currently available in AIT QKD “R10” is a new revamped version of Cascade with better Shannon efficiency, Enkey (turning key data BLOB into a AIT QKD keystream), Dekey (the reverse to Enky), qkd-statistics to collect statistical data during QKD pipeline processing and high level administration tool “qkd-pipeline” which supports auto-connecting the QKD modules on each side. This is accompanied with improved versions of error-estimation and tools for log data gathering and performance analysis. A dedicated simulator allows creating a stream of pseudo quantum events modelled around a broad set of variables like fiber length, signal loss, error probability, detector dark count rate and more.

The design of the AIT QKD “R10” software has been done with extensibility, flexibility and robustness in mind. Each module in the pipeline can be easily substituted with implementations of recently developed algorithms by independent teams without touching the rest of the pipeline. Therefore Quantum Bit-Commitment und Quantum-Coin-Flip protocols can be integrated assembling the pipeline with off-the-shelf modules and dedicated ones, as needed.

The AIT QKD “R10” QKD software is bundled with management tools, partly GUI oriented, based on Distributed Bus (DBus) message exchange technology to simply script QKD modules or AIT QKD based applications with Python or even Bash. Utilities and tools as well as a boilerplate setup for QKD module coding projects can be used to create new QKD post processing modules or QKD based user applications. Development stages of new projects utilizing the AIT QKD software, ranging from debugging support of parallel and distributed concurrently running QKD modules up to configuration, packaging and deployment, are presented.