New release of an open source QKD software: design and implementation of new algorithms, modularization and integration with IPSec

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

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

Introduction

Quantum Key Distribution (QKD) involves in a first step a physical exchange of quantum signals between a pair of devices, which can be carried out in numerous different ways. Whatever the realization of this "physical layer" of QKD is, it outputs a pair of strongly correlated bit strings. The latter have then to be distilled by a fundamentally universal classical, post-processing protocol to yield Information Theoretically Secure (ITS) keys. Post-processing communication requires communication channel authentication, itself using key material. Key management in well defined crypto contexts is therefore a must for ITS post processing operation. Moreover real world QKD systems need to be seamlessly integrated in standard communication and to inter-operate with higher level applications providing communication security.

This poster outlines the new design of the QKD software architecture and implementation by AIT, which addresses simultaneously all these issues while still being easy extensible and adoptable to novel techniques and algorithms in the context of QKD.

QKD Pipeline

A **QKD Pipeline** realizes quantum key distillation ranging from the detected signals up to a shared secret series of bits: the quantum key. Starting with QBit signal acquisition each **QKD Module** concentrates on a dedicated task: sifting, error correction, ...
Finally the shared secret keys are stored inside a Key Store which alongside a Crypto Engine provides means to directly extract keys from the system via "key pumps". Additionally a VPN can be feed by quantum keys.

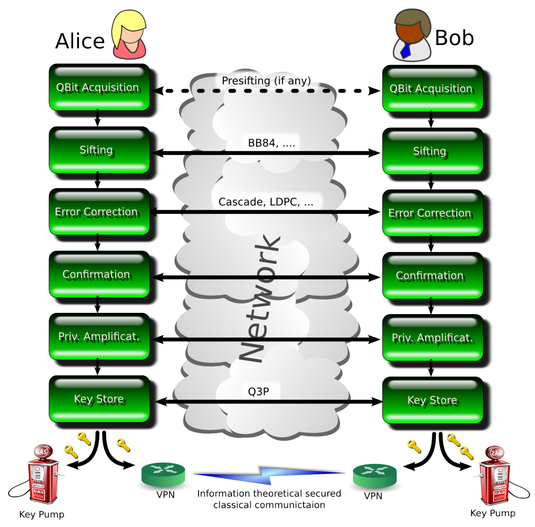

Figure 1: AIT QKD Pipeline

QKD Module

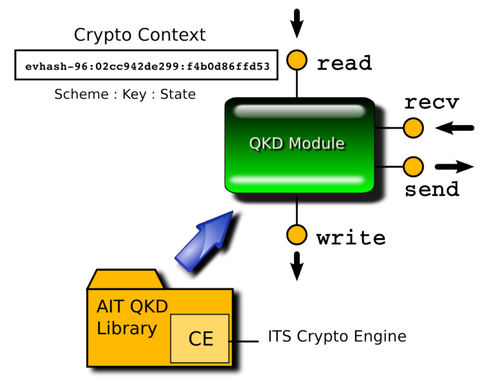

Figure 2: QKD Module

The building block of a QKD pipeline is a single QKD Module. Such modules are incorporated as UNIX processes.
The AIT QKD Library provides all functions for communication: from/to the next QKD Module, from/to the peer QKD Module. All these functions are mimicked as POSIX calls.
With the help of ready-to-use ITS crypto functions the AIT QKD Software environment enables ITS authenticated communication channels with the peer QKD Module during post processing.
Any QKD Module may change the current crypto setup during key distillation at will by instantiating new crypto contexts and finalizing the old one.

Software architecture

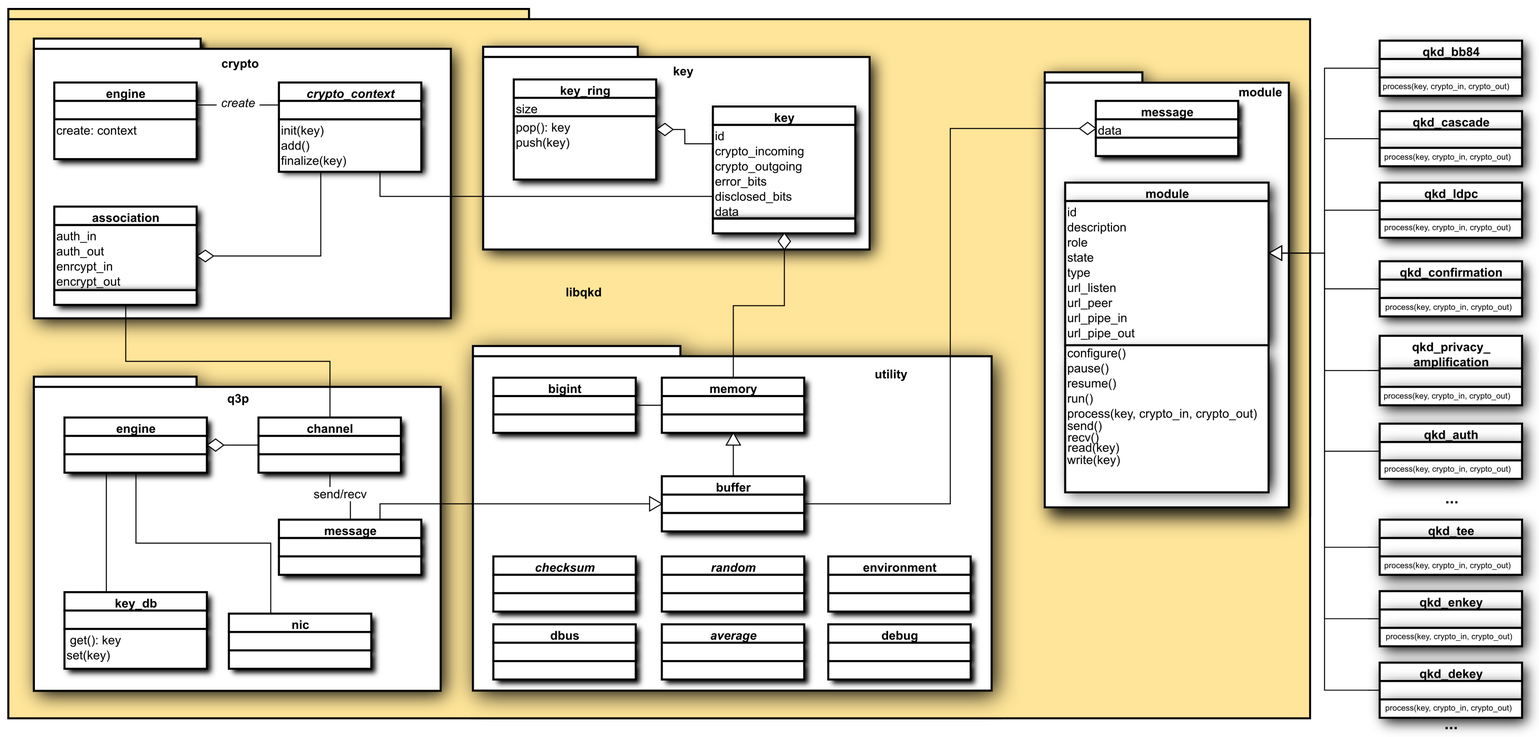

Figure 3: AIT QKD Software UML

The software architecture centers the AIT QKD library - **libqkd**: all essential data types and tools for QKD post processing containing key definition, crypto algorithms and **Q3P** (Quantum Point-to-Point Protocol) integration along QKD Module declarations. Each concrete QKD Module dedicated to a single specific task like sifting or error correction is then derived from the general QKD Module definition of the libqkd and fulfill its task by simply overriding the `process()` method. This isolates the detailed algorithm implementation inside the derived classes in their own process space. All network operations, QKD Module interconnection, and crypto algorithms are already implemented and available with ease.
The implementation is driven by the new possibilities of the recent **C++11** standard and well known software engineering design patterns. Keeping the interfaces of abstract classes small enables developers to introduce new implementations of frequently used parts like new crypto algorithms or integration of arbitrary random number hardware devices.

IPSec and ITS Network Integration

A Q3P engine connects to a single peer Q3P engine and enforces ITS communication in between. A trusted repeater is then realized by bundling multiple Q3P engine instances inside a **Q3P Node**. Each Q3P engine instance creates a dedicated new **virtual network interface card (NIC)** to be associated with an IP address thus creating an ITS meshed network accessible by today's network aware applications.

Due to the QKD key demand of Q3P links an **IPSec** connection can be created by utilizing the QKD keys stored at each Q3P engine and feeding these keys via the `setkey` Linux kernel call to update IPSec SA/SP databases at high rate. As these keys are generated by the QKD devices the IPSec integration does not need to run IKE based on classical keys agreement protocols.

Distribution and License

The AIT QKD post processing software is **Open Source**. The library is placed under LGPL V2.1 and accompanying binaries under GPL V2. Researchers are welcome to implement their own post processing entity. AIT maintains the AIT SQT QKD **Software Platform** containing the software, an issue tracker, wiki, and serves as a discussion platform for new ideas and development. Access to the software platform is charged with € 2000,- once.
The AIT QKD R10 Developer Snapshot 1 is free for download w/o registration via git with "`git clone http://sqt.ait.ac.at/git/qkd-public.git`"

Dual licensing policy, to be negotiated on demand, allows also for closed source developments and projects.

References

- AIT SQT QKD Software platform, https://sqt.ait.ac.at/software
- M. Peev et al., "The SECOQC Quantum Key Distribution Network in Vienna", New Journal of Phys., 11, 075001 (2009).