



Development of a Global Network for Secure
Communication based on Quantum Cryptography
www.secoqc.net

SECOQC-QBB-Link Interface

Publication

Announcement, General Description, Software Installation Instructions

Version:	0.014
Date:	01/05/2008
Reference:	
Author:	Thomas Länger, Austrian Research Centers – ARC GmbH
Status:	published
Related Documents:	SECOQC_QBB-LI_documentation.zip sourcecode.tar, i386_DEB.tar, i386_RPM.tar x86_64_amd64_DEB.tar, x86_64_amd64_RPM.tar

1 Contents

1	Contents	2
1.1	Contact.....	2
2	Press Announcements	3
2.1	Announcement - German.....	3
2.2	Announcement - English.....	3
3	Configuration – Overview	5
4	Published Items.....	7
5	Compatibility Issues	9
5.1	Release Information.....	9
5.2	Hardware and Software Prerequisites	9
5.3	Installation Instructions	10
6	Licenses and Terms of Use	12
6.1	Creative Commons ‘by-nc-nd’ 3.0 License	13
6.2	Creative Commons ‘by’ 3.0 License	14

1.1 Contact

The published binaries and source code, as well as the related documentation can be downloaded from SECOQC’s official homepage www.secoqc.net.

If you need to contact us, please send an email to the following address:

secoqc-if@arcs.ac.at

Austrian Research Centers GmbH, ARC
Business unit Quantum Technologies
Vienna / Austria

2 Press Announcements

2.1 Announcement - German

Veröffentlichung des SECOQC Quanten-Back-Bone Link-Interfaces

Die Partner des europäischen Projekts SECOQC, vertreten durch den Projekt-Koordinator Austrian Research Centers GmbH, ARC, freuen sich, die Veröffentlichung des im Rahmen des Projekts entwickelten SECOQC Quanten-Back-Bone Link Interfaces zur freien Benutzung, anzukündigen. Mit Hilfe dieses Interface können Quantenkryptographie-Links in das SECOQC Quantenkryptographie-Netzwerk eingefügt werden.

Die vollständige Dokumentation des Interfaces, sowie ein Softwarepaket mit einem Netzwerk-Knoten-Simulator, werden ab sofort auf der offiziellen SECOQC Projektseite www.secoqc.net zum Download angeboten.

Die Veröffentlichung des Interfaces richtet sich vor allem an die Entwickler von Quantenkryptographie-Links, die ihre Systeme gegen dieses Interface entwickeln können. Dadurch werden die Links mit dem SECOQC Netzwerk kompatibel und können ohne weiteres in das Netzwerk eingefügt werden. Während der Entwicklung kann der im Softwarepaket enthaltene Netzwerk-Knoten-Simulator verwendet werden, wodurch der Aufwand für Entwicklung, Testen und Validierung erheblich reduziert werden kann. Im Rahmen des Projekts SECOQC wurden fünf technologisch verschiedene Typen von Quantenkryptographie-Links entwickelt, die zu dem SECOQC Quanten-Back-Bone Interface kompatibel sind.

Die veröffentlichte Software kann auch ohne echten Quantenkryptographie-Links verwendet werden, um ein SECOQC Netzwerk mit mehreren Knoten und Quanten-Links zu simulieren.

Voraussetzung für die Installation ist ein Linux Betriebssystem (i386 oder x86_64/amd64 Plattform). Die Installationspakete werden in den Formaten für DEB-basierte Systeme (Debian, Ubuntu...) und RPM-basierte Systeme (Red Hat, SuSE...) zur Verfügung gestellt.

2.2 Announcement - English

Publication of SECOQC Quantum-Back-Bone Link-Interface

The participants of the European Integrated Project SECOQC of the 6th framework programme, represented by the co-ordinator Austrian Research Centers GmbH - ARC, are proud to announce the publication of the Quantum-Back-Bone Link-Interface QBB-LI. By this interface quantum cryptographic links can be inserted into the SECOQC Quantum Back Bone secrets distribution network.

Published is the complete interface documentation, as well as a software package including a network node simulator and a sample quantum device.

Target audience of this publication are developers of quantum cryptographic links who can use the provided simulation software as classical back-end to their systems. This makes their systems compatible to the SECOQC network and reliefs them of implementing a classical channel module and thus enables straightforward implementation and convenient testing and validation of the quantum optical systems and associated key distillation software. In SECOQC, five technologically different types of quantum cryptographic links were developed against the QBB-LI using the network node simulator.

The published software package can also be used without actual quantum cryptographic links to simulate a SECOQC quantum key distribution network with an arbitrary number of network nodes and quantum cryptographic links.

The software package requires a Linux operating system and is provided for DEB-based systems (Debian, Ubuntu,...) and RPM-based systems (Red hat, SuSE,...) for i386 and x86_64/amd64 platforms.

The documentation and software packages can be downloaded from the official SECOQC web site at www.secoqc.net.

3 Configuration – Overview

The SECOQC Quantum-Back-Bone Link Interface (QBB-LI) is located inside the node of the SECOQC QBB, exactly between the QBB-Links modules and the QBB-Node-Module, where in the following figure, Fig. 1, the ‘Communication Router’ is situated.

Physically, the QBB-Link and the QBB-Node-Module are connected by an Ethernet/TCP connection. This allows multiple possibilities for the configuration of the published components: It is likewise possible that the interface library, as well as the simulator run on the same computer as the key distillation protocol processor of the quantum link device, or that any of these run on separate machines in the same subnet.

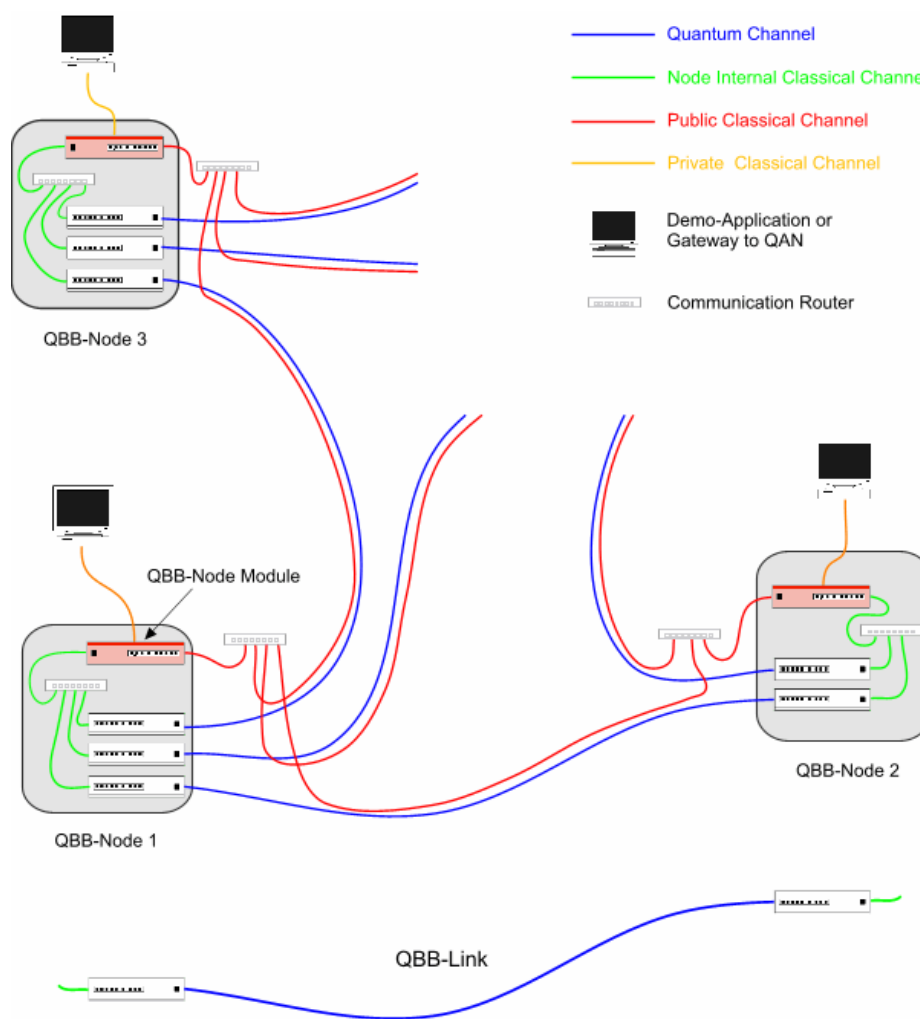


Fig. 1: Components of the SECOQC Quantum-Back-Bone QBB

Please note, that in Fig. 1 the (red) public channel is depicted as parallel structure to the (blue) quantum channels. This is how the public channel is physically implemented in the SECOQC demonstrator network. Any other topology of the public net is also feasible (In other diagrams the public network is often symbolised by an ‘internet-cloud’)

For an closer overview of the involved components (of the QBB-Node and the QBB-Link) and the location of the Interface see also the following figure:

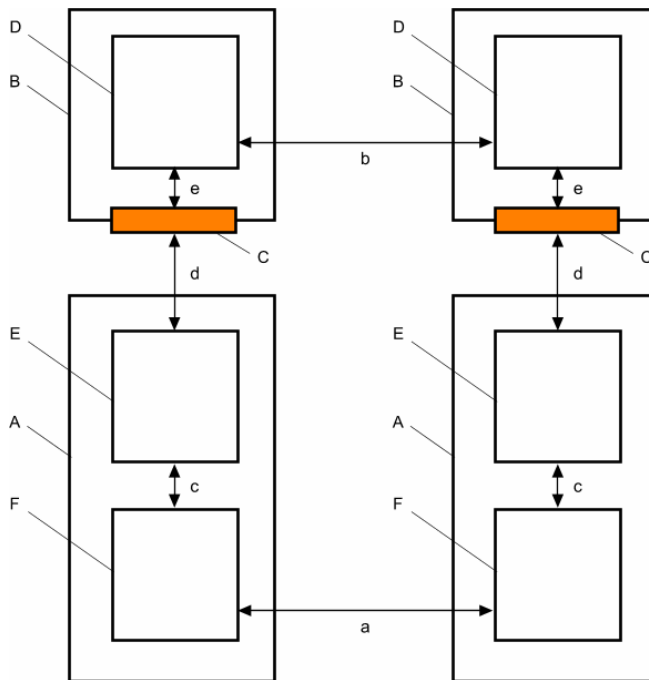


Fig. 2: SECOQC QBB-Node / QBB-Link Interface.

- A: Alice or Bob module of a QBB-Link
- B: QBB-Node module or QBB Node Simulator
- C: Quantum-Back-Bone Link Interface (QBB-LI)
- D: Q3P Component
- E: QKD distillation protocol processor
- F: Quantum optical setup
- a: Quantum channel
- b: Classical channel
- c: Raw key channel
- d, e: Connections to QBB-Node / QBB-Link Interface

The Q3P Components (D) of the QBB-Node modules (B) provides a public channel for the respective QKD distillation protocol processors (E) of the Alice and the Bob side of a QBB-Link. This channel can be used to transmit messages in one of the following four modes: plain, encrypted, authenticated, encrypted and authenticated – encryption and authentication are performed in an information theoretically secure way using one-time-pad, and universal-2-hash functions. Furthermore, the Q3P Components (D) take over the keys produced by the Alice- and Bob-modules.

4 Published Items

The SECOQC Quantum-Back-Bone Link Interface (QBB-LI) is a logical interface, which is realised electrically over an Ethernet connection. There are no principal objections to having the interface implemented in another technology. Ethernet was merely chosen in the SECOQC project because of its availability in computing platforms that are used by the SECOQC QBB-Link development teams in the prototypes they are producing for the demonstrator QBB network.

The following items shall be published as SECOQC Standard and made available for public use:

q3p-dev 0.4 - the SECOQC QBB Q3P C Library

This is the library which has to be linked to the protocol processor software of the QBB-Link in order to access the functionality of the QBB-Node. The q3p item contains:

- documentation
- compiled library

qd 0.2 - the SECOQC QBB sample quantum device

This is a sample QBB-Link protocol processor, demonstrating the use of the q3p functions. The qd software (qd for quantum device) is linked against the q3p library. The qd item comprises:

- source code
- documentation

simulator 0.3.1 – the SECOQC QBB Node-Simulator

The simulator (the word is a combination of ‘simulator’ and ‘emulator’) simulates a QBB network node from the point of view of the QBB-Link. The simulator completes the software package to be published so that a functioning system can be achieved without any addition. The simulator package contains:

- compiled and linked binary
- documentation

if-info 0.4.3 Interface Information

Interface information service – Utility for retrieving the interface configuration of the local system. The package contains

- compiled and linked binary
- documentation

yp 0.1.4 yellow pager daemon

The yellow pager announces available services in the local network segment. It enables the involved 'parties' (i.e. instances of the simulator) to find their respective counterparts without the need for manually setting configuration information. The package contains:

- compiled and linked binary
- documentation

5 Compatibility Issues

5.1 Release Information

The published package was distributed internal to SECOQC as release R2 'Faraday' in May 2006. Current release is R5 'Bohr' of summer 2007. R2 was the last release containing the simulator package, and was therefore selected for publication. All later releases already contain the fully functional 'real' SECOQC Quantum Back Bone node.

Since R2 the interface was subject to slight modifications, so that function calls may differ by their name and parameters. Yet, the functionality did not change and the upgrade of R2 compatible device software to the most recent release is supposed to be achievable with small effort.

5.2 Hardware and Software Prerequisites

Reference operating system is Debian GNU/Linux 4.0 "Etch", Kernel 2.6.22.9.

The following software packages versions were are recommended with the indicated version (or higher):

autoconf (GNU Autoconf) 2.61
Copyright (C) 2006 Free Software Foundation, Inc.

automake (GNU automake) 1.10
Copyright 2006 Free Software Foundation, Inc.

make (GNU Make) 3.81
Copyright (C) 2006 Free Software Foundation, Inc.

gcc (GCC) 4.1.2
Copyright (C) 2006 Free Software Foundation, Inc.

glibc-2.6.1

6 Installation Instructions

The distribution is provided for DEB-based systems (Debian, Ubuntu,...) and RPM-based systems (Red hat, SuSE,...) for i386 and x86_64/amd64 platforms. The following files will have to be downloaded for the respective platforms:

i386, RPM:

if-info-0.4.4-2.i386.rpm
yp-0.1.5-2.i386.rpm
q3p-dev-0.4.1-2.i386.rpm
simulator-0.3-3.i386.rpm
qd-0.2.1-2.i386.rpm

x86_64/amd64, RPM:

if-info-0.4.4-2.x86_64.rpm
yp-0.1.5-2.x86_64.rpm
q3p-dev-0.4.1-2.x86_64.rpm
simulator-0.3-3.x86_64.rpm
qd-0.2.1-2.x86_64.rpm

i386, DEB:

if-info-0.4.4_i386.deb
yp-0.1.5_i386.deb
q3p-dev-0.4.1_i386.deb
simulator-0.3_i386.deb
qd-0.2.1_i386.deb

x86_64/amd64, DEB:

if-info-0.4.4_amd64.deb
yp-0.1.5_amd64.deb
q3p-dev-0.4.1_amd64.deb
simulator-0.3_amd64.deb
qd-0.2.1_amd64.deb

The following packages contain the source of the SECOQC QBB sample quantum device. This file can be adapted and modified for testing and prototyping of own quantum optical hardware and key distillation protocol

source code:

qd-0.2.1-2.src.rpm
qd-0.2.1.tar.gz

The integrity of the packages can be verified by comparing md5 sums of the packages against the target hash values which can be downloaded from the same source.

The documentation is included in the packages. Detailed documentation on the interface is to be found in the q3p_dev documentation.

The following file is a startup script for launching an example network (with three nodes and six links)

startup script:

startup

Using suitable package management software, the packages are to be installed in the following order:

1. ifinfo
2. yp
3. q3p-dev
4. simulator
5. qd

Afterwards, the sample startup script can be used for an initial run of the software.

7 Copyright, Licenses, and Terms of Use

The copyright of the software remains with the Austrian Research Centers, ARC GmbH, as employer of the software authors.

Documentation and the compiled binaries of

- q3p-dev 0.4
- simulator 0.3.1
- if-info 0.4.3
- yp 0.1.5

are released under Creative Commons 'by-nc-nd' (Attribution, Non-commercial, No Derivatives) license, while the source code for the example quantum device protocol processor

- qd 0.2

is published under Creative Commons 'by' (Attribution) license.

It shall be noted, that contrary to documentation, for which the Creative Commons organisation explicitly encourages CC licensing, it discourages from using their licenses for software (see FAQ on [creativecommons.org](https://creativecommons.org/faq) for details). CC suggests using specific software licenses, as there are Free Software Foundation's GPL and LGPL. Yet, neither of these licenses is applicable on compiled binaries.

An alternative would have been to use one of the numerous available freeware licenses for the software but we were not able to identify a suitable one for our case. So, instead of inventing one more possibly problematic freeware license, we decided to release under CC anyway, because this suits well to the CC licensed documentation and displays in clear terms the conditions under which the items may be used: Attribution, Non-commercial, No Derivatives. Moreover, these conditions are implicitly upheld because of technical reasons (Except for q3p-dev, attribution is always displayed by software when it is executed; the software is not suitable for commercial application as some essential functionality is only stubbed and simulated; Derivatives are not possible as the software is distributed as binary only).

7.1 Creative Commons 'by-nc-nd' 3.0 License

This is the license for the documentation and the compiled binaries.

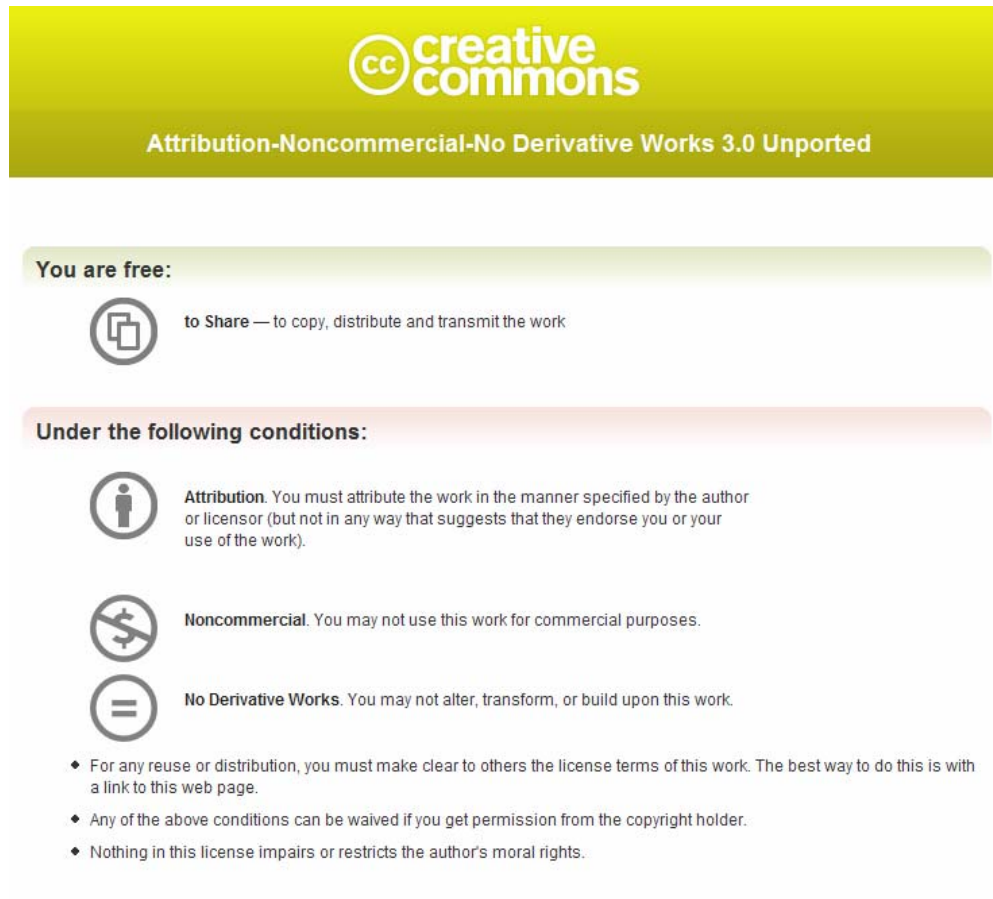


Fig. 3 Creative Commons by-nc-nd Summary

Screenshot of <http://creativecommons.org/licenses/by-nc-nd/3.0/> displaying the human-readable summary of the legal code (the full license) which can be retrieved from <http://creativecommons.org/licenses/by-nc-nd/3.0/legalcode>

7.2 Creative Commons 'by' 3.0 License

This is the license for the source code of the sample quantum device.

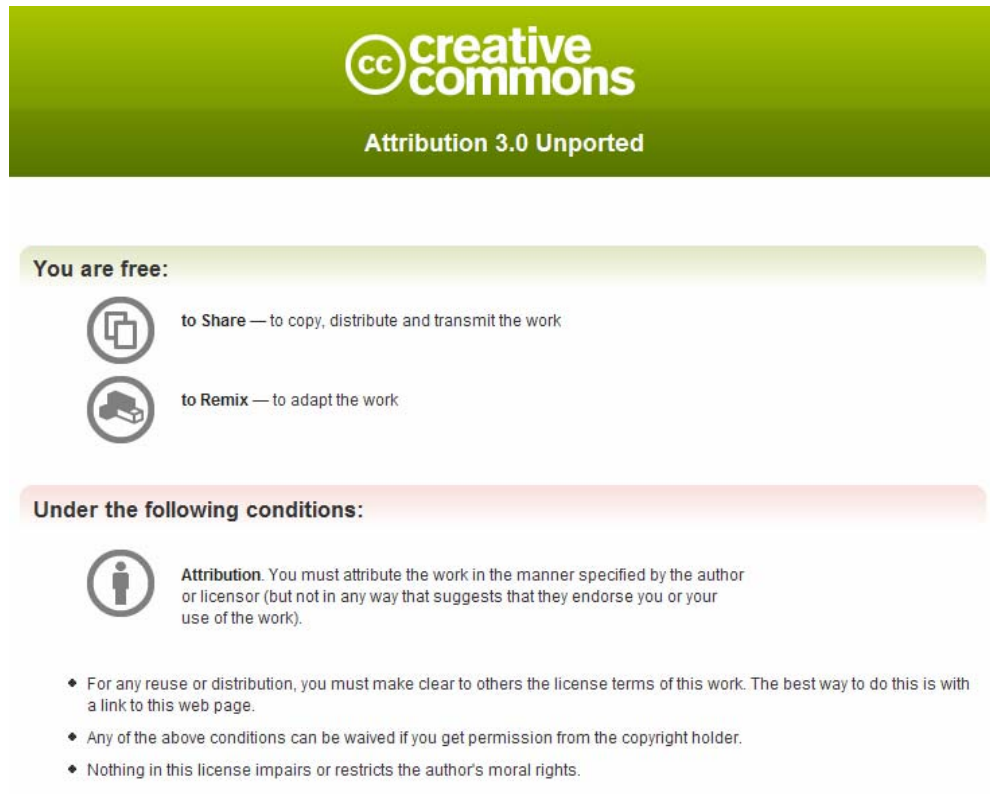


Fig. 4 Creative Commons 'by' Summary

Screenshot of <http://creativecommons.org/licenses/by/3.0/> displaying the human-readable summary of the legal code (the full license) which can be retrieved from <http://creativecommons.org/licenses/by/3.0/legalcode>

+++