ETSI GS QKD 005 V1.1.1 (2010-12)

Group Specification

Quantum Key Distribution (QKD); Security Proofs

Disclaimer

This document has been produced and approved by the Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG. It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/QKD-0005_SecProofs

Keywords
protocol, Quantum Key Distribution, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification (ISG) Group Quantum Key Distribution (QKD).

Introduction

The present document shall define the generic requirements for quantum information theoretic security proofs of quantum cryptography. It shall serve as a reference for the construction of requirements and evaluation criteria for practical security evaluation of quantum key distribution (QKD) systems.

In contrast to conventional cryptography which is often based on computational assumptions, quantum cryptography, notably QKD, offers "unconditional security" based on the laws of physics. To deliver such promise, demonstrating security by means of a security proof is an important aspect of quantum cryptography. Security proofs of quantum cryptography and their applicability have to be addressed with extreme care and precision primarily for two reasons. First, the security definition of a quantum cryptographic *protocol* is rather subtle. Second, it is often challenging to enforce assumptions in a security proof of a quantum cryptographic protocol in a practical quantum cryptographic *system*. Notice that any seemingly minor or innocent violation of an assumption in a security proof might be exploited by an adversary with disastrous consequences on the security of a practical QKD system.

The above two points:

i) the subtlety in security definitions; and

ii) the challenges to enforce assumptions in a practical QKD system,

shall be the two main themes of the present document.