

## 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.

<https://standards.iteh.ai>  
Document Preview

[ETSI GS QKD 005 V1.1.1 \(2010-12\)](https://standards.iteh.ai/catalog/standards/etsi/049534e9-8e14-4e04-ab86-63ca3b869303/etsi-gs-qkd-005-v1-1-1-2010-12)

<https://standards.iteh.ai/catalog/standards/etsi/049534e9-8e14-4e04-ab86-63ca3b869303/etsi-gs-qkd-005-v1-1-1-2010-12>



## 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

(<https://standards.iteh.ai>)  
Document Preview

**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/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/ETSI_support.asp)

**Copyright Notification**

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2010.  
All rights reserved.

**DECT**<sup>TM</sup>, **PLUGTESTS**<sup>TM</sup>, **UMTS**<sup>TM</sup>, **TIPHON**<sup>TM</sup>, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

**3GPP**<sup>TM</sup> is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**LTE**<sup>TM</sup> is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

**GSM**<sup>®</sup> and the GSM logo are Trade Marks registered and owned by the GSM Association.

# Contents

Intellectual Property Rights .....	4
Foreword.....	4
Introduction .....	4
1 Scope .....	5
2 References .....	5
2.1 Normative references .....	5
2.2 Informative references .....	5
3 Definitions, symbols and abbreviations .....	6
3.1 Definitions .....	6
3.2 Symbols .....	9
3.3 Abbreviations .....	9
4 Security Definition .....	9
4.1 What QKD delivers .....	9
4.2 Structure of QKD protocols.....	10
4.3 Framework for Security Statements of QKD Implementations.....	10
4.4 Scientific Security proof framework .....	12
4.4.1 Security Assumptions on Devices .....	12
4.4.2 Assumptions on Adversary .....	12
4.5 Modelling, Assumptions and Side Channels .....	13
4.5.1 Source .....	14
4.5.2 Detection unit .....	15
4.6 Classical assumptions (shielding, electronic side-channels) .....	15
4.7 Classical protocol .....	15
4.7.1 Sifting .....	16
4.7.2 Error estimation .....	16
4.7.3 Error Correction (Reconciliation) .....	16
4.7.4 Confirmation.....	17
4.7.5 Privacy Amplification.....	17
4.7.6 Authentication.....	17
4.7.7 Common Sources of Mistakes in Classical Protocols.....	18
<b>Annex A (informative): Authors &amp; contributors.....</b>	<b>20</b>
History .....	21

---

# 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.