QKD security from BSI‘s perspective

Tobias Hemmert (BSI)

Insights on QKD & QKDN certification: Recent developments and challenges

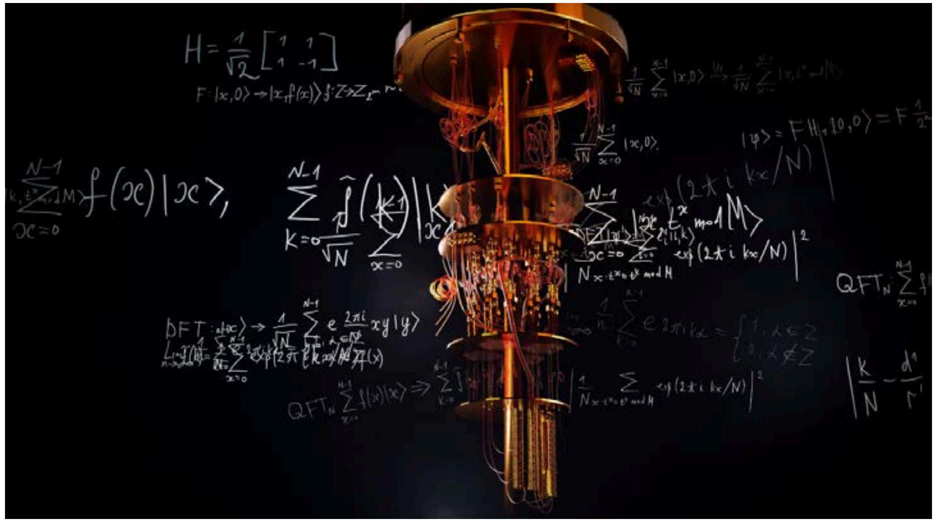
Singapore, 17/05/2024

Federal Office
for Information Security

The need for quantum-safe cryptography

BSI‘s working assumption (not a forecast) for high-security applications:

With non-negligible probability, there will be a cryptographically relevant quantum computer by the beginning of the 2030s.



Source: *© Ulia Koltyrina / Adobe Stock*

ANSSI, BSI, NLNCSA, Swedish NCSA

Position Paper on QKD

- On a theoretical level, QKD can provide information-theoretic security.
- For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice.
- QKD is not yet sufficiently mature from a security perspective.

→ The clear priorities should be the migration to PQC and/or the adoption of symmetric keying.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office
for Information Security

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

SWEDISH ARMED FORCES

Position Paper on Quantum Key Distribution

French Cybersecurity Agency (ANSSI)
Federal Office for Information Security (BSI)
Netherlands National Communications Security Agency (NLNCSA)
Swedish National Communications Security Authority, Swedish Armed Forces

Executive summary

Quantum Key Distribution (QKD) seeks to leverage quantum effects in order for two remote parties to agree on a secret key via an insecure quantum channel. This technology has received significant attention, sometimes claiming unprecedented levels of security against attacks by both classical and quantum computers.

Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective. In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying.

This paper is aimed at a general audience. Technical details have therefore been left out to the extent possible. Technical terms that require a definition are printed in italics and are explained in a glossary at the end of the document.

ANSSI, BSI, NLNCSA, Swedish NCSA

Why QKD is not sufficiently mature: Selected issues

- No standardised QKD protocols
- No comprehensive security proofs under realistic conditions
- Evaluation methodology (e.g. to evaluate resistance against implementation attacks) missing

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office
for Information Security

General Intelligence and
Security Service
Ministry of the Interior and
Kingdom Relations

SWEDISH ARMED FORCES

Position Paper on Quantum Key Distribution

French Cybersecurity Agency (ANSSI)
Federal Office for Information Security (BSI)
Netherlands National Communications Security Agency (NLNCSA)
Swedish National Communications Security Authority, Swedish Armed Forces

Executive summary

Quantum Key Distribution (QKD) seeks to leverage quantum effects in order for two remote parties to agree on a secret key via an insecure quantum channel. This technology has received significant attention, sometimes claiming unprecedented levels of security against attacks by both classical and quantum computers.

Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective. In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying.

This paper is aimed at a general audience. Technical details have therefore been left out to the extent possible. Technical terms that require a definition are printed in italics and are explained in a glossary at the end of the document.

Theoretical security:
Protocol standardization and security proofs

Standardization of cryptographic schemes…

… is crucial for security because:

- Slight modifications of secure cryptographic schemes can render them insecure.

- Even experienced cryptographers and security experts make mistakes in designing secure protocols.

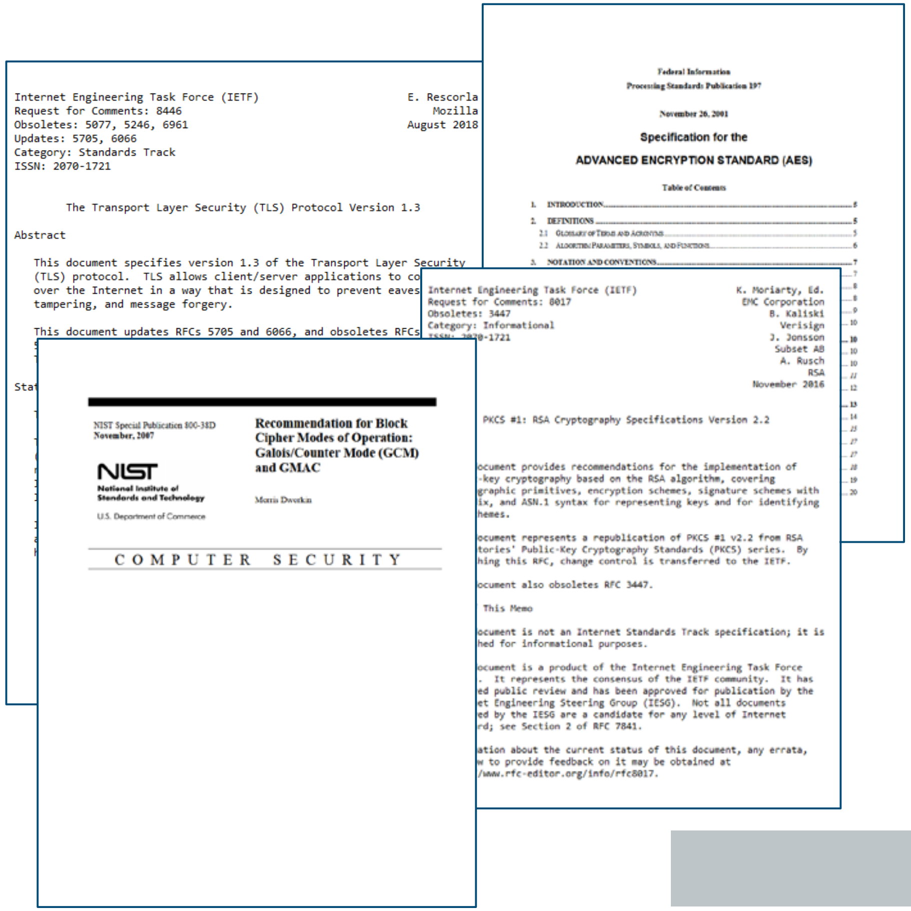
Standards provide clear specifications of cryptographic schemes that have been vetted by many experts.

Standardization of classical cryptography

- All widely-used cryptographic primitives and protocols have been standardized by a standards organization.

- The standards have been scrutinized by the community.

- It is widely accepted to only rely on standardized cryptographic schemes.



Internet Engineering Task Force (IETF)   E. Rescorla
Request for Comments: 8446   Mozilla
Obsoletes: 5077, 5246, 6961   August 2018
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to co
over the Internet in a way that is designed to prevent eaves
tampering, and message forgery.

This document updates RFCs 5705 and 6066, and obsoletes RFCs

Stat

Federal Information
Processing Standards Publication 197

November 26, 2001

Specification for the

ADVANCED ENCRYPTION STANDARD (AES)

Table of Contents

1. INTRODUCTION 5
2. DEFINITIONS 5
2.1 GLOSSARY OF TERMS AND ACRONYMS 5
2.2 ALGORITHM PARAMETERS, SYMBOLS, AND FUNCTIONS 6
3. NOTATION AND CONVENTIONS 7

Internet Engineering Task Force (IETF)   K. Moriarty, Ed.
Request for Comments: 8017   EMC Corporation
Obsoletes: 3447   B. Kaliski
Category: Informational   Verisign
ISSN: 2070-1721   J. Jonsson
                                                                 Subset AB
                                                                  A. Rusch
                                                                       RSA
                                                             November 2016

PKCS #1: RSA Cryptography Specifications Version 2.2

ocument provides recommendations for the implementation of
-key cryptography based on the RSA algorithm, covering
graphic primitives, encryption schemes, signature schemes with
ix, and ASN.1 syntax for representing keys and for identifying
hemes.

ocument represents a republication of PKCS #1 v2.2 from RSA
tories' Public-Key Cryptography Standards (PKCS) series. By
hing this RFC, change control is transferred to the IETF.

ocument also obsoletes RFC 3447.

This Memo

ocument is not an Internet Standards Track specification; it is
hed for informational purposes.

ocument is a product of the Internet Engineering Task Force
. It represents the consensus of the IETF community. It has
ed public review and has been approved for publication by the
et Engineering Steering Group (IESG). Not all documents
ed by the IESG are a candidate for any level of Internet
rd; see Section 2 of RFC 7841.

ation about the current status of this document, any errata,
w to provide feedback on it may be obtained at
/www.rfc-editor.org/info/rfc8017.

NIST Special Publication 800-38D
November, 2007

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

Morris Dworkin

COMPUTER SECURITY

Standardization of QKD protocols?

So far, no QKD protocol has been standardized by a standards organization.

The need for standardized QKD protocols and security proofs

QKD products will most likely not be adopted for sensitive applications or achieve certification without

- the use of **standardized QKD protocols** (e.g. decoy-state BB84), plus
- matching **security proofs**

that have been widely scrutinized by experts.

This is only the baseline for secure QKD products, implementation security is also crucial.

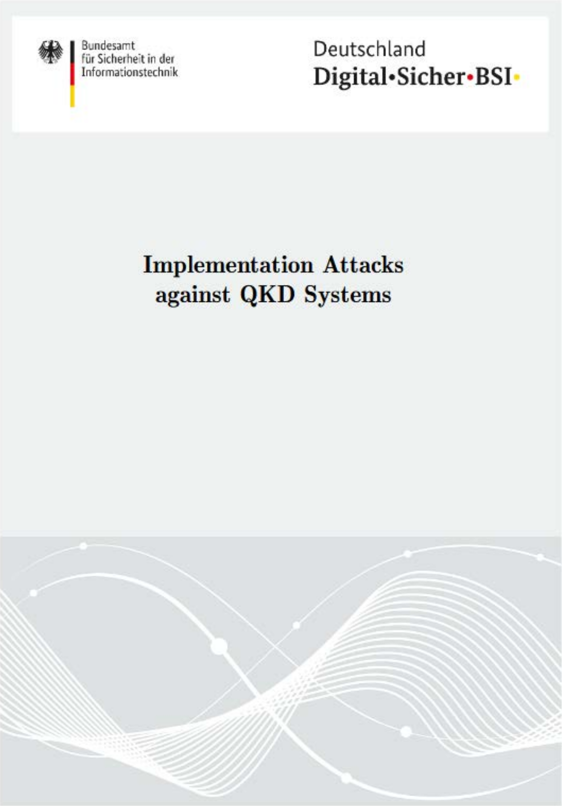
Implementation security and certification

BSI report on implementation attacks

- Structured overview of known QKD-specific implementation attacks on QKD systems according to the literature

Some open challenges for the QKD community:

- Research on further attacks
- Effectiveness of countermeasures?
- More practical attack experience
- „Classical“ IT security of QKD devices



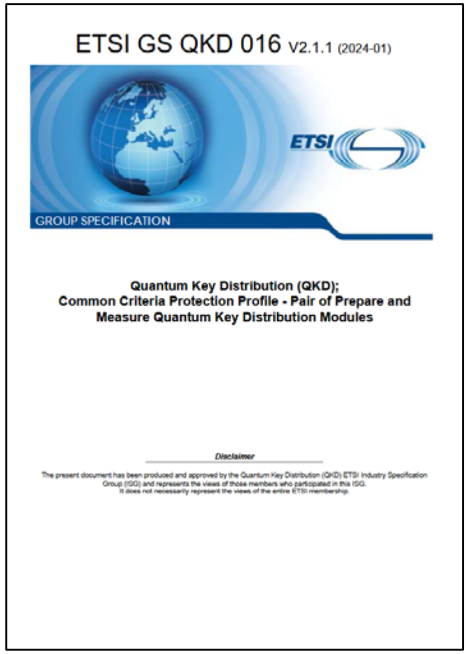
Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Implementation Attacks
against QKD Systems

Source: BSI webpage

Towards QKD certification



ETSI GS QKD 016 V2.1.1 (2024-01)

**Quantum Key Distribution (QKD);
Common Criteria Protection Profile - Pair of Prepare and
Measure Quantum Key Distribution Modules**

Disclaimer

The present 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.

ISO/IEC 23837
(parts 1 and 2)

Security requirements, test and evaluation methods for quantum key distribution

Many standards are still missing to achieve certification of QKD devices, see for example:

- Presentations by Dirk Fischer (BSI) in ETSI ISG QKD
- CEN/CENELEC Standardization Roadmap on Quantum Technologies

Conclusion: QKD security from BSI‘s perspective

- The development of quantum computers threatens communication security today.
- Our priority should be the migration to post-quantum cryptography.

In order to obtain assurance about the security of QKD devices:

- Standardized QKD protocols with matching associated security proofs are required.
- More research on implementation attacks and countermeasures is required.
- Evaluation criteria and more standards for certification need to be further developed.

Further information: www.bsi.bund.de/Quanten