ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

QKD standardization in ISO/IEC JTC 1/SC 27

- An introduction of ISO/IEC 23837

Hongsong Shi

China information technology security evaluation center

ITU workshop on quantum information technology for networks

Shanghai, China

2019/6/7

Background

- **ISO/IEC JTC 1/SC 27 - *Information security, cybersecurity and privacy protection***
  - The development of standards for the protection of information and ICT

181	67	49	29
published ISO standards* under the direct responsibility of ISO/IEC JTC 1/SC 27	ISO standards under development* under the direct responsibility of ISO/IEC JTC 1/SC 27	Participating members	Observing members

Working Groups

ISO/IEC JTC 1/SC 27/WG 1	Information security management systems
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies

https://www.iso.org/committee/45306.html

Outline

- Background
- Motivation
- Structural analysis

Background

- In 2007, the standardization of QKD device in ISO/IEC was launched as a study period project first
- In April of this year, ISO/IEC JTC1/SC27 approved a new work item, numbered ISO/IEC 23837
  - Information technology —Security Techniques —Security requirements, test and evaluation methods for quantum key distribution
- Two parts are scheduled

ISO/IEC 23837-1: Requirements
Jiajun Ma
Andrew Shields,
Charles Ci Wen Lim

ISO/IEC 23837-2: Test and evaluation methods
Hongsong Shi, Martin Ward,
Gaetan Pradel

  - It is now in WD1 phase, and expected to be published in 2022

Motivation

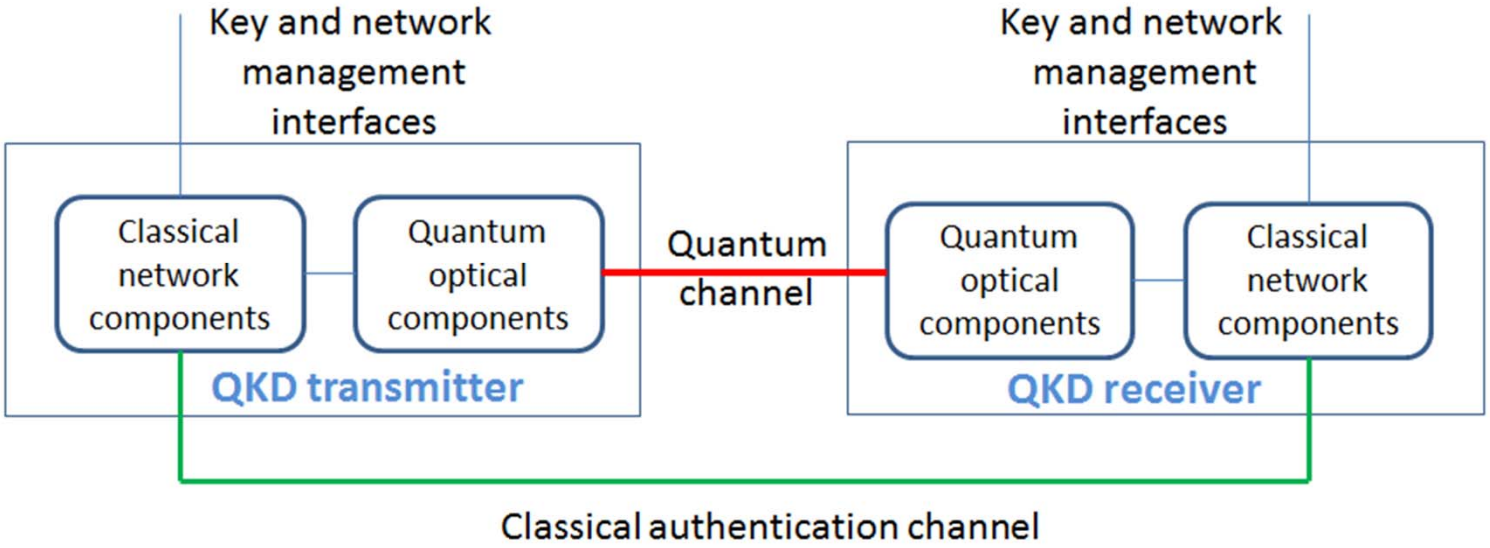
- ISO/IEC 23837 is built on the top of the Common Criteria, and will shape the framework of security evaluation of QKD module

- Security problem definition,
- Security functional requirements,
- security evaluation activities

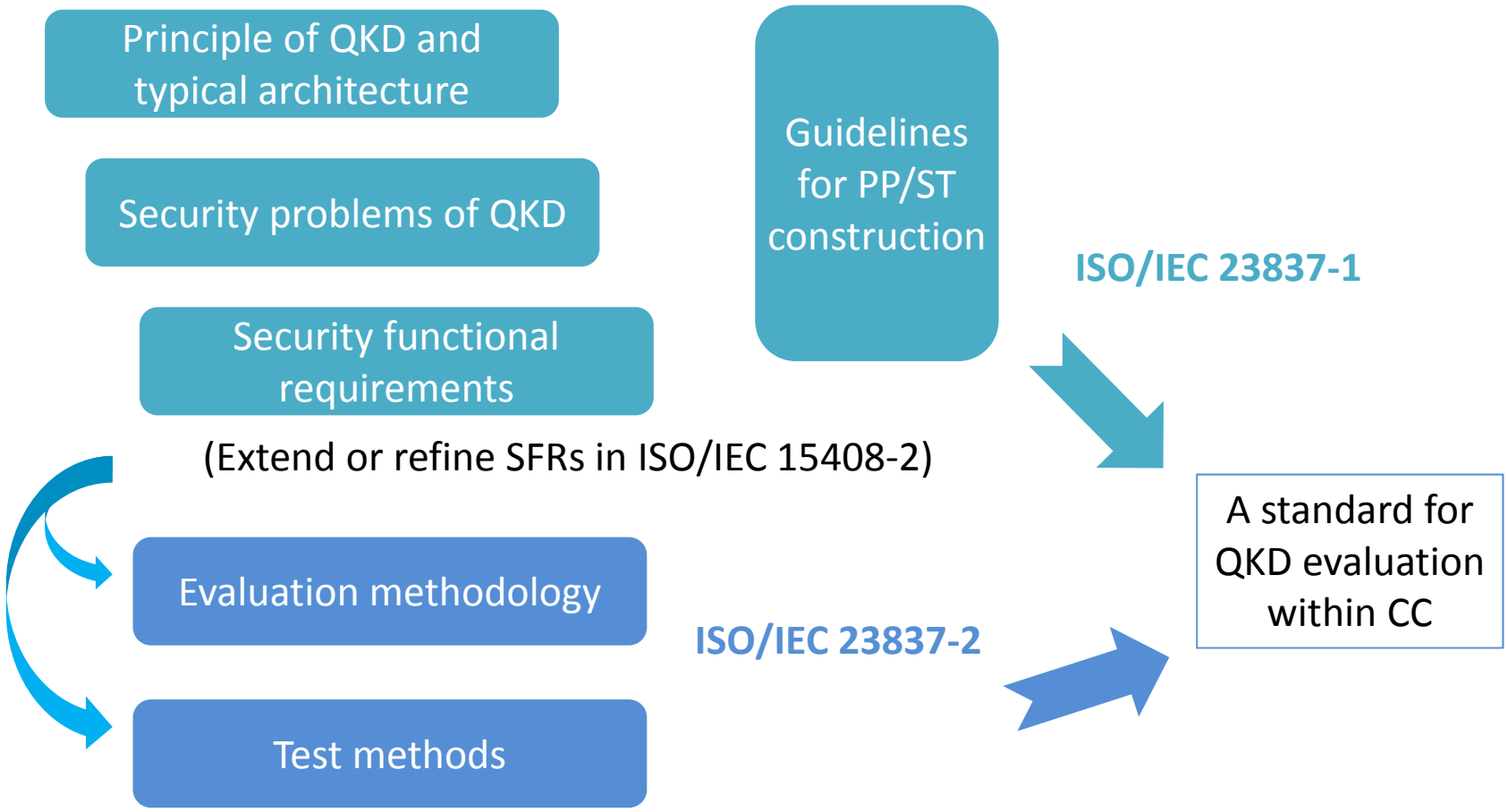
  - Serve as a basis for PP/ST construction
  - A high-level standard to provide a general framework for QKD evaluation
  - No evaluation assurance level will be specified, but the evaluation activities for functional testing and vulnerability assessment （under EAL5） will be specified
    - PP/ST can specify the required EALs, and the standard can provide supporting activities

Scope of the standard

- On QKD device
  - What requirements should be met for a QKD device to be secure?
  - How to validate the satisfiability of the requirements?



General structure of the standard



Principle of QKD and typical architecture

The theoretical aspects of QKD

QKD Implementation

- **Principle of QKD**
  - The objective
  - The channels
- **Theoretical security model of QKD**
  - ε-security definition
  - Security proof model
- **Classification of QKD protocols**
  - *Improve the generality of the standard*
  - CV, DV protocols
  - Prepare-and-measure, MDI, entanglement-based protocols
- **Architecture of QKD systems**
  - Typical architectures of different protocols

Principle of QKD and typical architecture

The theoretical aspects of QKD

QKD Implementation

- **External interfaces of QKD module**
  - The quantum channel + classical auth channel *(computationally unbounded attacks)*
  - System management interface + key management interface *(computationally bounded attacks)*
- **Internal structure of QKD module**
  - The composition of QKD module
  - Classical network components + quantum optical components
- **General working flow of QKD system**
  - Pre-processing, raw-key communication, post-processing, system calibration

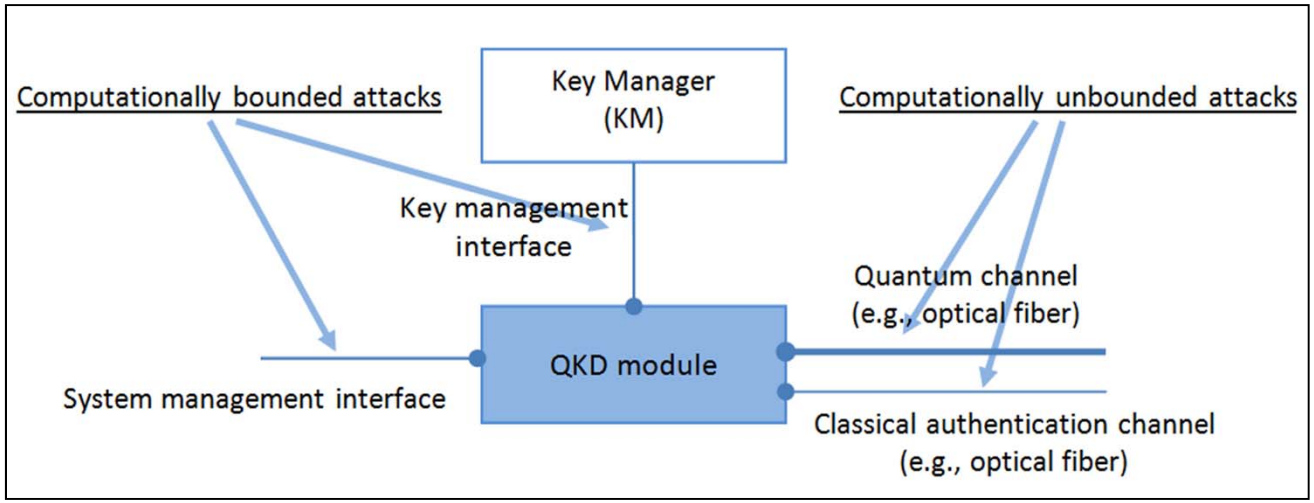
Security problems of QKD

Assumptions on the operational environment

Asset protected by QKD device

Threats to classical network components

Threats to quantum optical components



Security problems of QKD

Assumptions on the operational environment

Asset protected by QKD device

Threats to classical network components

Threats to quantum optical components

- **Quantum mechanics is complete in describing adversarial actions to QKD**
  - Computationally bounded + unbounded attackers
- **Developers and operators are trusted**
  - No backdoor
  - Follow security policy to operate
- **The platform that QKD functionality resides is secure**
  - OS + hardware are trusted
- **External sensitive data and credential are protected**
- **The device is physically protected in its operational environment**
  - Classical side channel attacks will not be considered in the standard
  - Assume environmental protection

Security problems of QKD

Assumptions on the operational environment

Asset protected by QKD device

- **Final key and all intermediate key material** should be protected
- **The TOE security functionality** should be protected from misusing

Threats to classical network components

Threats to quantum optical components

Security problems of QKD

Assumptions on the operational environment

Asset protected by QKD device

Threats to classical network components

Threats to quantum optical components

- **Unauthorized access**
  - Circumvent the access control mechanism and access CSP or keys, of misuse TSF
- **Cryptographic analysis**
  - Exploit the vulnerabilities in crypto algorithms and their implementation
- **Randomness defect**
- **Functions abuse**
  - Abuse functions which may not be used after TOE delivery or life-cycle phase transition
- **Failure exploitation**
- **Audit circumvention**
- **Malicious update**

Security problems of QKD

Assumptions on the operational environment

Asset protected by QKD device

Threats to classical network components

Threats to quantum optical components

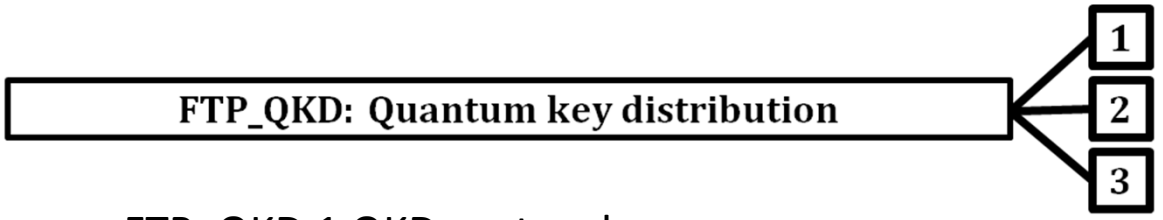
- **Threats exploiting optical source flaws**
  - exploit the flaws of quantum-state-preparation-related units (including signal source and encoder) of the transmitter to violate the security of QKD
- **Threats exploiting optical detection flaws**
  - exploit the flaws of quantum-state-detection-related units (including decoder and detector) of the receiver to to violate the security of QKD
- **Threats exploiting other flaws**
  - exploit the flaws in the pre-processing phase, post-processing or calibration phase to violate the security of QKD

Security functional requirements

Extended security functional components

Security functional requirements of QKD

- **Principle for component extension**
  - If some security objectives of QKD cannot be translated or is difficult to be translated to the pre-defined functional components in CC part



- FTP_QKD.1 QKD protocol
- FTP_QKD.2 Post-processing of QKD
- FTP_QKD.3 Calibration of QKD

Security functional requirements

Extended security functional components

Security functional requirements of QKD

8.4.2.5 FTP_QKD.1 QKD protocol

Component relationships

Hierarchical to:	No other components.
Dependencies:	FTP_QKD.2 Key generation by QKD

FTP_QKD.1.1
The TSF shall implement [*assignment: quantum key distribution protocol*] acting as [*assignment: defined protocol role(s)*] in accordance with: [*assignment: list of standards*] to achieve [*selection, choose one of: information theoretic security, long-term security*].

FTP_ QKD.1.2
The TSF shall permit [*selection: itself, its peer*] to initiate communication via the secure channel.

FTP_ QKD.1.3
The TSF shall employ one of the following mechanisms: [*assignment: list of information theoretic secure message authentication schemes*] in accordance with: [*assignment: list of standards*] to authenticate the network traffic over the classical authentication channel with its peer, in order to achieve [*selection, choose one of: information theoretic security, long-term security*].

FTP_ QKD.1.4
The TSF shall enforce the following static protocol options: [*assignment: list of options and references to standards in which each is defined*].

FTP_ QKD.1.5
The TSF shall negotiate one of the following protocol configurations with its peer: [*assignment: list of configurations and reference to standards in which each is defined*] over the classical authentication channel.

Security functional requirements

Extended security functional components

Security functional requirements of QKD

- **The approach**
  - Commonly required security functional requirements (SFRs) will be identified and specified based on the extended and pre-defined components

- **Security functional requirements for** *classical network components*
- **Security functional requirements on** *quantum-state-preparation components*
- **Security functional requirements on** *quantum-state-detection components*
- **Security functional requirements on** *post-processing procedure*
- **Security functional requirements on** *calibration procedure*

Security functional requirements

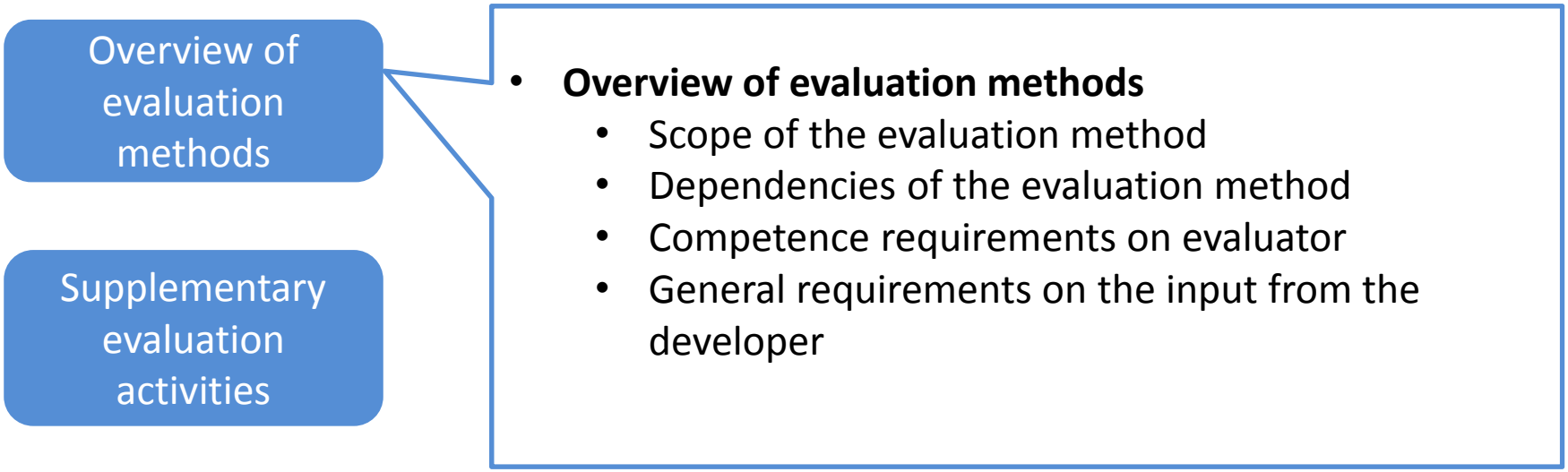
Extended security functional components

Security functional requirements of QKD

Exceptions

- If existing components are sufficient to be used, components extension won't be considered
- For generality of the standard, only extensively required SFRs will be given, those requirements from specific protocols will not be considered in principle

Security evaluation and test methods



Security evaluation and test methods

Overview of evaluation methods

Supplementary evaluation activities

- **Supplementary activities to ISO/IEC 18045 on functional testing (ATE) (under ISO/IEC 15408-4)**
  - Supplementary activities to the evaluation of classical network components
    - Objective of evaluation activity
    - Required inputs
    - Required tool types and setup
    - Rationale
    - Test procedure
    - Pass/fail criteria
  - Supplementary activities to the evaluation of *quantum-state-preparation* components
  - Supplementary activities to the evaluation of *quantum-state-detection* components
  - Supplementary activities to the evaluation of *calibration* procedure
- **Supplementary activities to ISO/IEC 18045 on Vulnerability assessment (AVA)**

Security evaluation and test methods

Overview of evaluation methods

Supplementary evaluation activities

Test item	Description
Photon-number distribution	Test if the quantum source emits single photon. Characterize the photon-number distribution of the source.
State encoding accuracy	Test if the degree of freedom of the optical pulses (e.g., polarization) used for encoding are properly modulated as required in the protocol. Characterize the difference between the practical and ideal modulation.
State preparation consistency	Test if the degrees of freedom other than the encoding one of the optical pulses (e.g., spectral, temporal, spatial degree of freedom) are consistently prepared in the same states. Characterize their difference between different pulses.
Indistinguishability of prepared states	Test if the features of the non-encoding degrees of freedom are indistinguishable. Characterize the distinguishability between different quantum states on the non-encoding degrees of freedom.
Isolation of the quantum-state-preparation	Test if optical laser is prevented from being injected into the quantum-state-preparation modules. Characterize the isolation of the injected laser whose power is limited by the maximum transmitted power

Security evaluation and test methods

Overview of evaluation methods

Supplementary evaluation activities

- **Supplementary activities to ISO/IEC 18045 on Vulnerability assessment (AVA)**
  - Components claimed to achieve computational security objective
  - Components with information theoretic security assurance
  - The whole system can be validated to meet the requirements of the intended security assurance level
- **Refinement of the factors for the calculation of attack potential**
  - **Identification of vulnerabilities**
    - corresponds to the effort required to create the attack, and to demonstrate that it can be successfully applied
  - **Exploitation of vulnerabilities**
    - corresponds to achieving the attack on another instance of the TOE in its intended operational environment using the analysis and techniques defined in the identification phase
  - **Factors refinement**
    - Elapsed time, expertise, knowledge of the TOE, window of opportunity, equipment

Security evaluation and test methods

Overview of evaluation methods

Supplementary evaluation activities

Table D.1 — Calculation of attack potential

Factor	Value	
	Identification	Exploitation
Elapsed Time		
<= one day	0	0
<= one week	1	2
<= two weeks	2	4
<= one month	4	8
> one month	8	16
Expertise		
Layman	0	0
Proficient	2	4
Expert	4	8
Multiple experts	8	Not applicable
Knowledge of TOE		
Public	0	Not applicable
Restricted	2	Not applicable
Sensitive	4	Not applicable
Critical	8	Not applicable
Window of Opportunity (Access to TOE)		
Easy	0	0
Moderate	2	4
Difficult	4	8
Window of Opportunity (Access to Biometric Characteristics)		
Immediate	Not applicable	0
Easy	Not applicable	2
Moderate	Not applicable	4
Difficult	Not applicable	8
Equipment		
Standard	0	0
Specialised	2	4
Bespoke	4	8

Security evaluation and test methods

Overview of evaluation methods

Supplementary evaluation activities

Table D.2 — Rating of vulnerabilities and TOE resistance

Values	Attack potential required to expoit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components:	Failure of components:
< 10	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-19	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
20-29	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
30-39	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>40	Beyond-High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Security evaluation and test methods

Overview of evaluation methods

Supplementary evaluation activities

Considerations

- The standard will not specify the expected evaluation assurance levels (EALs) for QKD, but rather to supplement all the required assurance activities for QKD evaluation, such that EAL based evaluation (under EAL 5) can be performed

Collaboration

The editorial team consists of experts from different countries

- With all-around experience in QKD/classical crypto research and security evaluation
- The editing work will be done through cooperation with world-wide experts
- Cooperation will be required to resolved the collected comments before and during each working group meeting of ISO/IEC JTC1/SC27

Collaboration with ITU-T SG17 is under way

- ISO/IEC 23837 can be regarded as a complementary work to the QKD network standardizations in ITU-T SG17
- Liaison has been built between the two sides
- Editing material will be circulated through the liaison channel
- Experts from ITU-T SG17 are solicited to review the documents and make contributions

Thank you