ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 47679.2—2026/ISO/IEC 23837-2:2023

网络安全技术　量子密钥分发的安全要求、测试和评估方法　第2部分:测试和评估方法

Cybersecurity technology—Security requirements, test and evaluation methods for quantum key distribution—Part 2: Test and evaluation methods

(ISO/IEC 23837-2:2023, Information security—Security requirements, test and evaluation methods for quantum key distribution—Part 2: Evaluation and testing methods, IDT)

2026-05-25 发布　　2026-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 47679《网络安全技术　量子密钥分发的安全要求、测试和评估方法》的第2部分。GB/T 47679已经发布了以下部分:

——第1部分:要求;

——第2部分:测试和评估方法。

本文件等同采用ISO/IEC 23837-2:2023《信息安全　量子密钥分发的安全要求、测试和评估方法　第2部分:评估和测试方法》。

本文件做了下列最小限度的编辑性改动:

——为与现有标准协调,将标准名称改为《网络安全技术　量子密钥分发的安全要求、测试和评估方法　第2部分:测试和评估方法》;

——为与现有标准协调,第1章增加附加信息,明确本文件的适用范围;

——删除了ISO、IEC术语数据库网址;

——为提升标准文件的可读性,补充ADV、AGD、APE、ASE、ATE、FSP、FTP、ST等缩略语。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:科大国盾量子技术股份有限公司、中国信息安全测评中心、中国科学技术大学、合肥国家实验室、中电信量子信息科技集团有限公司、中国人民解放军国防科技大学、中山大学、中国电子科技集团公司第三十研究所、安徽问天量子科技股份有限公司、正则量子(北京)技术有限公司、北京量子信息科学研究院、华为技术有限公司、中国电子技术标准化研究院、北京天融信网络安全技术有限公司、中国信息通信研究院、上海循态量子科技有限公司、广东国腾量子科技有限公司、国科量子通信网络有限公司、安徽华创鸿度光电科技有限公司、中移雄安信息通信科技有限公司、信通数智量子科技有限公司、中国电信集团有限公司、广西大学、中国人民解放军网络空间部队信息工程大学、国家信息技术安全研究中心、兴唐通信科技有限公司、吉林信息安全测评中心、中国长城科技集团股份有限公司、北京邮电大学、深圳市纽创信安科技开发有限公司、中移(苏州)软件技术有限公司、中国电子信息产业集团有限公司第六研究所、麒麟软件有限公司、中国电子科技集团公司第十五研究所、广州仁合时创信息技术有限公司、深圳市旭子科技有限公司。

本文件主要起草人:唐世彪、石竑松、李东东、刘宏伟、王振、黄安琪、孙仕海、廖胜凯、赵梅生、王立伟、刘婧婧、徐兵杰、汤艳琳、林阳荟晨、魏伟、王天宇、黄蕾蕾、赖俊森、束庆邦、于庆军、刘波、谭昊、施婷婷、李政宇、周颖明、武宏宇、吴允祝、王宇航、饶华一、张维杨、于宗文、凌杰、张启发、陈烨、魏士慧、李雪莹、张静、李华生、郭邦红、谢欢文、李振华、窦天琦、范元滨、杨洋、刘春池、韦克金、马海强、李宏伟、王卓、汪洋、王肖斌、姚飞、王龙、王子涛、缪亚军、李明翰、黄伟、于春霖、刘占丰、葛晓航、邹超、王宗岳、刘健、董晶晶、李艳俊、张大朋、杨诏钧、朱奕、王永峰。

引　言

GB/T 47679《网络安全技术　量子密钥分发的安全要求、测试和评估方法》在GB/T 18336(所有部分)的框架下,确立了量子密钥分发(QKD)模块的安全要求、测试和评估方法。本文件主要规定了QKD模块通用安全评估方法及相应评估活动,包括对GB/T 47679.1—2026中QKD模块相关安全功能要求(SFR)的补充评估活动,以及针对安全保障等级(EAL)1至EAL 5+的安全保障要求(SAR)的补充评估活动。

GB/T 47679拟由两部分构成。

——第1部分:要求。目的在于确立QKD模块安全评估的一般性框架,并给出QKD模块通用基线SFR集。

——第2部分:测试和评估方法。目的在于确立QKD安全评估的测试和评估方法,给出针对QKD协议、QKD模块中量子光学部件及传统网络部件的SFR所构成的测试与评估方法的评估活动,并给出安全保障要求的补充评估活动,以符合相应保障级QKD的安全评估。

本文件给出了QKD协议实现,以及QKD发送方模块和接收方模块中量子光学部件的测试和评估活动。对于传统网路部件特有的SFR,本文件未规定具体评估活动,主要参考网络设备的现有评估方法。同时,本文件明确了安全保障要求的补充评估活动,并对GB/T 30270—2024中的通用脆弱性分析方法进行了细化,涵盖攻击潜力计算的指南。

本文件目的在于为QKD制造商提升QKD模块的设计与实现安全性提供技术规范,指导评估方开展QKD模块的测试和安全评估工作,从而降低QKD系统运行中因安全功能失效所带来的风险。

网络安全技术　量子密钥分发的安全要求、测试和评估方法　第2部分:测试和评估方法

1　范围

本文件确立了量子密钥分发(QKD)安全评估的测试和评估方法,规定了针对QKD协议实现、QKD模块中量子光学部件及传统网络部件的安全功能要求所构成的测试与评估方法的评估活动,并给出了安全保障要求的补充评估活动,以支持相应保障级QKD的安全评估。

本文件适用于QKD相关产品的研制、开发、测试和评估。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.4—2024　网络安全技术　信息技术安全评估准则　第4部分:评估方法和活动的规范框架(ISO/IEC 15408-4:2022, IDT)

GB/T 30270—2024　网络安全技术　信息技术安全评估方法(ISO/IEC 18045:2022, IDT)

GB/T 47679.1—2026　网络安全技术　量子密钥分发的安全要求、测试和评估方法　第1部分:安全要求(ISO/IEC 23837-1:2023, IDT)

3　术语和定义

GB/T 47679.1—2026界定的以及下列术语和定义适用于本文件。

3.1

衰减　attenuation

光波在传输媒介中传播时,其强度随传输距离增加而减弱的物理量。

3.2

衰减器　attenuator

用于降低光波功率的装置。

3.3

反向荧光　back-flash

单光子探测器产生的单个或多个光子脉冲。

注1:这种现象也称为“回闪”或“击穿荧光”。

注2:这种现象是由辐射性电荷复合引发,常见于雪崩光电二极管等电子-空穴对大量生成的器件中。

3.4

分束器　beam splitter (BS)

按设计比例将入射光波分为二束或多束独立光波的装置。