ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T 47679.1—2026/ISO/IEC 23837-1:2023

# 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1部分:要求

**Cybersecurity technology—Security requirements, test and evaluation methods for quantum key distribution—Part 1: Requirements**

**(ISO/IEC 23837-1:2023, Information security—Security requirements, test and evaluation methods for quantum key distribution—Part 1: Requirements, 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1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 23837-1:2023《信息安全　量子密钥分发的安全要求、测试和评估方法　第1部分:要求》。

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1部分:要求》;

——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。

——删除了第3章ISO、IEC术语数据库网址。

——为提升本文件的可读性,第4章增加FUN_KM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:中国信息安全测评中心、科大国盾量子技术股份有限公司、中国科学技术大学、合肥国家实验室、中国人民解放军国防科技大学、中山大学、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、中电信量子信息科技集团有限公司、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、中国电子科技集团公司第三十研究所、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、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、中国网络空间研究院、北京数字认证股份有限公司、中国电子科技集团公司第十五研究所、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、广州仁合时创信息技术有限公司。

本文件主要起草人:石竑松、王振、刘宏伟、黄安琪、孙仕海、唐世彪、廖胜凯、赵梅生、刘婧婧、黄蕾蕾、王立伟、魏伟、王天宇、刘云、林阳荟晨、张维杨、施婷婷、范元滨、李政宇、杨洋、李雪莹、赖俊森、徐兵杰、黄伟、周颖明、方昊、王宇航、饶华一、李东东、汤艳琳、郭邦红、谢欢文、戚巍、李明翰、李振华、窦天琦、韦克金、李宏伟、汪洋、魏士慧、于宗文、刘占丰、闻明、吴嘉杰、马海强、王卓、武宏宇、吴允祝、钱泳君、谭昊、刘春池、张超、张静、陈烨、邹超、王宗岳、姚飞、王肖斌、王龙、范晶、林浩、赵松、陈澍、霍姗姗、刘健、束庆邦、李小文、黄伟、吴一阳。

# 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)的安全要求,给出了相应的测试和评估方法。本文件主要规定了QKD模块通用基线安全功能要求(SFR)集。

GB/T 47679拟由两个部分构成。

——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。

理论上,QKD是一种通过预共享密钥生成长对称密钥的技术,其安全性不依赖于攻击者的算力;所生成的密钥能随后用于构建安全通信信道等密码应用场景。

尽管QKD协议的理论安全性已在严格的安全模型(假设通信双方预先共享安全密钥)下得到了证明,但理论模型与工程实现间的偏差往往会出现在QKD模块生存周期的各个阶段。这些偏差可能导致实际QKD系统出现安全漏洞。其中,严重的侧信道攻击已被提出,并且在QKD黑客攻击实验中已有一些原理性的验证演示。与传统密码模块及网络设备一样,QKD模块在投入实际应用前,期望通过严格的安全测试与评估,以防范安全攻击导致的信息泄露风险。在QKD被业界广泛认可前,细致且严格的安全评估是必不可少的一步。

为此,GB/T 47679为QKD模块制造商明确了严格统一的安全规范:制造商能依此开发基于QKD技术的IT产品;评估者能按此实施安全测试和评估,从而有效降低QKD系统运行中因安全功能失效带来的风险。本文件采用GB/T 18336(所有部分)中标准化的模型与描述语言,规定了QKD模块的通用基线SFR集,覆盖从传统网络部件到量子光学部件的QKD协议的全部实现。附录A提供了QKD模块的保护轮廓编制指南。GB/T 47679的第2部分则明确了QKD模块达到预期评估保障级所需的具体安全评估活动。

注:本文件对扩展安全功能组件(见8.2)和SFR(见第9章)的描述,在安全功能族、组件结构、文本格式(即黑体和粗体)等方面与GB/T 18336.2—2024的安全功能组件保持一致,这些样式是按照GB/T 18336.2—2024的约定进行描述的,以便将某些术语与其他文本区分开来。这种描述方式便于熟悉GB/T 18336(所有部分)的用户能应用扩展安全功能组件和SFR编制QKD模块的评估文档。

# 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:要求

## 1　范围

本文件依据GB/T 18336(所有部分)确立了QKD模块安全评估的一般性框架,并规定了QKD模块通用基线安全功能要求(SFR)集,包括传统网络部件与量子光学部件的SFR,以及QKD协议的实现。为促使SFR的分析,基于对QKD模块安全功能的结构分析和QKD协议分类,本文件分析了QKD模块在其运行环境中可能面临的安全问题。

QKD模块传统网络部件的SFR主要在GB/T 18336(所有部分)确立的框架下进行刻画,并依据ISO/IEC 19790的方法,以及密码模块和网络设备测试相关的标准。

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 18336.1—2024　网络安全技术　信息技术安全评估准则　第1部分:简介和一般模型(ISO/IEC 15408-1:2022,IDT)

GB/T 18336.2—2024　网络安全技术　信息技术安全评估准则　第2部分:安全功能组件(ISO/IEC 15408-2:2022,IDT)

## 3　术语和定义

GB/T 18336.1—2024界定的以及下列术语和定义适用于本文件。

3.1

**攻击者　adversary;attacker**

故意利用QKD系统(3.28)潜在脆弱性的实体。

[来源:GB/T 25069—2022,3.221,有修改]

3.2

**鉴别　authentication**

验证某一实体所声称身份的过程。

[来源:GB/T 25069—2022,3.296]

3.3

**经典信道　classical channel**

通信双方用于交互编码数据的通信信道,所交互的数据可被无损读取和完全复制。