ICS 35.040
CCS L 80

中华人民共和国国家标准

GB/T 45240—2025

器件无关量子随机数发生器通用要求

General requirements for device-independent quantum random number generators

2025-01-24 发布　　2025-08-01 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。

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。

本文件由全国量子计算与测量标准化技术委员会(SAC/TC 578)提出并归口。

本文件起草单位：济南量子技术研究院、安徽国科量子网络有限公司、中国科学技术大学、清华大学、科大国盾量子技术股份有限公司、中国信息安全测评中心、中国长城科技集团股份有限公司、安徽问天量子科技股份有限公司、山西大学、上海交通大学、山东国科量子通信网络有限公司、中国科学院上海微系统与信息技术研究所、中国科学院软件研究所、中国计量科学研究院、深圳市国信量子科技有限公司、北京中科国光量子科技有限公司、上海国盾量子信息技术有限公司。

本文件主要起草人：李明翰、江扬帆、王明磊、张强、张军、聂友奇、张行健、李东东、石竑松、刘宏伟、于春霖、吴嘉杰、刘婧婧、申恒、郁昱、戚巍、缪亚军、张伟君、曹伟琼、邓玉强、王一曲、赵义博、谢树欣。

器件无关量子随机数发生器通用要求

1 范围

本文件界定了器件无关量子随机数发生器的术语和定义，描述了器件无关量子随机数发生器的结构组成，规定了器件无关量子随机数发生器的性能要求。

本文件适用于器件无关量子随机数发生器的研制和检测。

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。

GM/T 0005—2021 随机性检测规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

贝尔不等式 Bell inequality

贝尔型不等式

一类用于检验节点间局域隐变量理论的不等式。

3.2

贝尔检验 Bell test

对是否满足**贝尔不等式**(3.1)进行的检验。

3.3

非信令条件 nonsignaling condition

对于没有相互通信的不同事件，其结果的分布需要满足的条件。

3.4

纠缠源 entanglementsource

所产生的粒子间存在量子纠缠的粒子源。

注 1：量子纠缠是指多个物理系统状态之间的一种非经典关联属性。

注 2：纠缠源具有不同类型，如基于光子、原子等。

3.5

量子态 quantum state

量子系统的状态。

[来源：GB/T 42565—2023，3.1]