《器件无关量子随机数产生器通用要求》
国家标准编制说明

（征求意见稿）

2024 年 5 月 24 日

目　录

《器件无关量子随机数产生器通用要求》
国家标准编制说明

一、工作简况

（一）任务来源及协作单位

2023 年 3 月 21 日，国家标准化管理委员会发布《关于下达 2023 年第一批推荐性国家标准计划及相关标准外文版计划的通知》（国标委发〔2023〕10 号），下达了《器件无关量子随机数产生器通用要求》推荐性国家标准的制定任务，计划号：20230192-T-469，任务周期 18 个月。本文件由全国量子计算与测量标准化技术委员会（SAC/TC 578）提出并归口管理，由济南量子技术研究院、国科量子通信网络有限公司、山东国科量子通信网络有限公司、安徽问天量子科技股份有限公司、科大国盾量子技术股份有限公司、深圳市国信量子科技有限公司、中国长城科技集团股份有限公司、北京中科国光量子科技有限公司、山西大学、上海交通大学、清华大学交叉信息研究院、中国信息安全测评中心、中国科学技术大学、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等单位共同负责标准起草。其中，济南量子技术研究院为该标准起草工作的牵头单位。

（二）制定背景

2020 年 10 月 16 日，中共中央总书记习近平在中央政治局第二十四次集体学习时强调，要充分认识推动量子科技发展的重要性和紧迫性，统筹基础研究、前沿技术、工程技术研发，培育量子通信等战略性新兴产业，抢占量子科技国际竞争制高点，构筑发展新优势。

在国家顶层布局和相关部委的大力支持下，我国量子信息技术整体处于国际领先地位，其中量子密钥分发和量子随机数技术在实用化方面发展最为突出，正处于从技术领先向产业综合领先发展的关键时期，急需标准化工作的指导。特别在中共中央、国务院于2021年10月印发的《国家标准化发展纲要》中，将“推动标准化与科技创新互动发展”放在五大任务之首，提出要加强关键技术领域标准研究，以科技创新提升标准水平，健全科技成果转化为标准的机制。《纲要》明确指出，要“在人工智能、量子信息、生物技术等领域，开展标准化研究……部分领域关键标准适度领先于产业发展平均水平。”

器件无关量子随机数产生器具备物理原理保障的随机性和与器件无关的特性，满足了随机数应用中对不可预测性和安全性的最高要求，具有广泛的应用需求。本文件对器件无关量子随机数产生器提出通用性要求，同时也给出器件无关量子随机数产生器的相关指标要求，对器件无关量子随机数的生产及使用提供指导和规范，促进该领域产业化应用的高质量发展。

（三）主要工作过程

2022年1月4日，济南量子技术研究院联合国科量子通信网络有限公司成立前期工作组，启动《器件无关量子随机数产生器通用要求》标准的起草准备工作；2022年5月6日，前期工作组向全国量子计算与测量标准化技术委员会（SAC/TC 578）提交了标准的立项申报资料；2022年6月12日，全国量子计算与测量标准化技术委员会（SAC/TC 578）全体委员投票表决通过立项申请（应参加投票委员人数54，实际参加投

票委员人数 52，同意 52，反对 0，弃权 0）； 2022 年 11 月 17 日，通过立项评估；2022 年 11 月 29 日，通过专业处审核；2022 年 12 月 22 日开始计划网上公示，至 2023 年 03 月 13 日，完成公示。

2022 年 12 月 13 日，国家标准化管理委员会批准立项申请，正式下达《器件无关量子随机数产生器通用要求》推荐性国家标准的制定任务，计划号：20230192-T-469，任务周期 18 个月。任务下达后，技术归口单位全国量子计算与测量标准化技术委员会（SAC/TC 578）会同项目牵头单位济南量子技术研究院，面向领域内相关科研院所、企事业单位、社会团体等，广泛开展了标准编写工作组成员单位/起草专家的征集工作。

2023 年 7 月 4 日，《器件无关量子随机数产生器通用要求》国家标准编写工作组正式成立。起草工作组由来自济南量子技术研究院、国科量子通信网络有限公司、清华大学、中国科学技术大学、上海交通大学、中国信息安全测评中心、山东国科量子通信网络有限公司、安徽问天量子科技股份有限公司、中国长城科技集团股份有限公司、山西大学、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共 15 个单位的 21 名专家组成。张强教授任组长，组员有李明翰、江扬帆、王明磊、刘洋、赵洪涛、刘婧婧、王一曲、陈柳平、于春霖、赵义博、申恒、张凯羿、石竑松、黄溢智、聂友奇、张伟君、曹伟琼、范靖云、张行健、邓玉强。

2023 年 7 月 4 日，工作组成立大会暨第一次工作组会议在济南召开，为“线上线下结合”的会议方式。会议由第一起草人国科量子通信网络

有限公司李明翰博士主持，济南量子技术研究院、国科量子通信网络有限公司、清华大学、中国科学技术大学、上海交通大学、中国信息安全测评中心、山东国科量子通信网络有限公司、安徽问天量子科技股份有限公司、中国长城科技集团股份有限公司、山西大学、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共15家单位的21位专家出席。会议进行了编写工作任务分工，制定了编写工作计划，并要求各单位对标准草案进行意见反馈。会议共收到国科量子通信网络有限公司、中国计量科学研究院、中国信息安全测评中心、中国科学技术大学、中国科学院软件研究所、安徽问天量子科技股份有限公司、清华大学、济南量子技术研究院、微系统所、中国长城科技集团股份有限公司、山西大学、深圳市国信量子科技有限公司等单位提出的修改意见53条。

2023年8月至2024年3月，工作组认真研究并完成了对53条意见的修改，形成讨论稿（第二稿），并将讨论稿（第二稿）发送给工作组全体成员单位研究，进一步提出修改意见。

2024年5月7日，工作组召开第二次工作会议，会议为线上会议。会议由第一起草人国科量子通信网络有限公司李明翰博士主持，济南量子技术研究院、国科量子通信网络有限公司、清华大学、中国科学技术大学、上海交通大学、安徽问天量子科技股份有限公司、中国长城科技集团股份有限公司、山西大学、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、北京中科国光量子

科技有限公司、科大国盾量子技术股份有限公司等 13 家单位的 20 位专家出席。会议同意科大国盾量子技术股份有限公司加入标准起草工作组。会议听取了国科量子通信网络有限公司针对征求意见的逐条回应和相应的修改结果，随后针对讨论稿（第二稿）的内容再次逐条讨论，征询意见。会议共收到修改意见 22 条。

2024 年 5 月，工作组完成对第二次会议收集的修改意见处理，形成讨论稿（第三稿），并将讨论稿（第三稿）发送给工作组全体成员单位。

2024 年 5 月 24 日，工作组召开第三次工作会议，会议为线上会议。会议由第一起草人国科量子通信网络有限公司李明翰博士主持，济南量子技术研究院、国科量子通信网络有限公司、清华大学、中国科学技术大学、上海交通大学、中国信息安全测评中心、山东国科量子通信网络有限公司、科大国盾量子技术股份有限公司、安徽问天量子科技股份有限公司、山西大学、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、北京中科国光量子科技有限公司 14 家单位的 16 位专家出席。会议首先听取了国科量子通信网络有限公司针对征求意见的逐条回应和相应的修改结果，随后针对讨论稿（第三稿）的内容再次逐条讨论，征询意见。会上，工作组 14 家成员单位通过腾讯会议投票功能进行投票表决，投票结果同意对工作组讨论稿（第三稿）修改完善后，形成征求意见稿和征求意见稿编制说明，向 TC578 标委会秘书处提交。投票情况：应参加投票单位 16 家，实际参加投票单位 14 家，同意 13 家，反对 0 家，弃权 1 家。

（四）国家标准主要起草人及其所做的工作

本文件由济南量子技术研究院作为牵头单位，国科量子通信网络有限公司、山东国科量子通信网络有限公司、安徽问天量子科技股份有限公司、科大国盾量子技术股份有限公司、深圳市国信量子科技有限公司、中国长城科技集团股份有限公司、北京中科国光量子科技有限公司、山西大学、上海交通大学、清华大学交叉信息研究院、中国信息安全测评中心、中国科学技术大学、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等单位共同负责标准起草。

二、国家标准编制原则、主要内容及其确定依据

（一）标准编制原则和依据

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，在标准技术要求的确定上，遵循以下原则：

1.在国内当前的技术条件下实现标准化目标具有完全可能性。

2.本项目的技术与主流技术发展方向相符合。

3.当前技术条件下标准可实现。

（二）标准主要技术内容说明

本文件描述了器件无关量子随机数产生器的术语和定义、结构组成、安全性要求等通用要求。

本文件适用于器件无关量子随机数产生器的研制和检测。

本文件的主要技术内容包括：1 范围、2 规范性引用文件、3 术语和定义、4 符号、5 器件无关量子随机数产生器结构组成、6 安全性要求。

（三）标准中主要技术内容确定的依据和过程

目前，国际上尚未有器件无关量子随机数产生器通用要求的相关规范或标准。为便于不同领域的研究人员能够准确地了解、使用本文件，本文件重点对器件无关量子随机数产生器通用要求的结构和功能进行介绍。在测试方法的步骤上，本文件方法建立过程中，综合考虑了当前国内外各课题组的技术路线以及各商业化公司的产品，对器件无关性检验要求做了详细介绍，保证试验方法的可操作性和可重复性。

三、试验验证情况的说明

本文件中涉及的验证实验数据见标准文档的附件及测试报告所示。

（一）主要试验的分析

本文件对器件无关量子随机数产生器器件无关性检验进行验证。

（二）主要试验验证的分析、综述报告

本文件使用的方法，经过国内外器件无关量子随机数产生器的重复使用，其有效性得到了充分的验证，基本可以统一器件无关量子随机数产生器通用要求，为行业推荐可操作的测试评估方法奠定基础。

（三）试验方案设计

- 试验对象准备：器件无关量子随机数产生器。
- 实验结果见试验验证报告。

（四）试验结果

基于上述验证试验数据的结果，可以得出结论：本文件在国内可以有效实施。

四、与国际、国外同类标准技术内容的对比情况

无。

五、标准采用国际文件的情况说明

无。

六、与有关的现行法律、法规和强制性国家标准的关系

经查，本文件与现有标准及制定中的标准无交叉重复，不涉及国内外专利，与有关的现行法律、法规和强制性国家标准无冲突。

七、制修订过程中是否存在重大分歧意见，以及重大分歧意见的处理过程

本文件制定过程中无重大分歧意见。

八、标准中涉及专利的情况

未发现涉及相关专利。

九、国家标准性质的建议及贯彻国家标准的要求和措施建议

鉴于本文件规定内容不涉及人身健康和生命财产安全、国家安全、生态环境安全等内容，属于基础性标准。根据标准化法及有关规定，建议本文件作为推荐性国家标准。

本文件的建议实施日期为：自发布之日起 6 个月。

本文件的实施，为我国器件无关量子随机数产生器通用要求提供了规范，不仅有助于明确系统术语定义、结构组成、功能要求、性能检验要求等通用要求，同时也给出器件无关量子随机数产生器的相关指标要求，对器件无关量子随机数的生产及使用提供指导和规范，促进该领域

产业化应用的高质量发展。

建议保证标准文本的充足供应，使各相关方能够及时获取标准文本。对于标准使用过程中容易出现的疑问，工作组做好必要、及时的解释工作。针对不同的使用对象，有侧重点地进行标准培训和宣贯，以保证标准的贯彻实施。

十、其他应予说明的事项

编写工作组承诺，本文件无版权风险。

《器件无关量子随机数产生器通用要求》国家标准编写工作组

2024 年 5 月 26 日

附件

《器件无关量子随机数产生器通用要求》

实验测试报告

1. 纠缠源

基于极化周期为 46.1816um 的 II 型 周期性极化磷酸氧钛钾晶体(PPKTP)的自发参量下转换过程，产生双光子对；设计 Sagnac 环结构，制备纠缠态。装置如图 1.1 所示，波长为 780nm 的泵浦脉冲光输入由偏振分束器（PBS）、半波片（HWP）、反射镜（RM）构成的 Sagnac 环，偏振分量$|H\rangle$顺时针方向经过 PPKTP 晶体进行自发参量下转换过程产生波长为 1560nm 的双光子对，偏振态分别为$|H\rangle_1$和$|V\rangle_2$，经过 45° HWP 后，偏振态为$|V\rangle_1$和$|H\rangle_2$；偏振分量$|V\rangle$逆时针方向经过 45° HWP 后，偏振态变为$|H\rangle$，经 PPKTP 晶体进行自发参量下转换过程产生双光子对$|H\rangle_1$和$|V\rangle_2$。下转换光子对在 PBS 处进行干涉，得到纠缠态：

$\cos 26.8^{o}\,|HV\rangle + \sin 26.8^{o}\,|VH\rangle$。

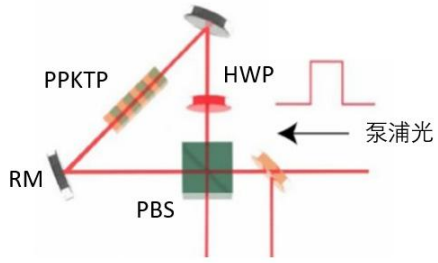

图 1.1 纠缠源

采用最大似然法进行量子态层析，对纠缠光子对的量子态进行重构，最终获得纠缠态保真度为 98.8%。结果如图 1.2 所示。

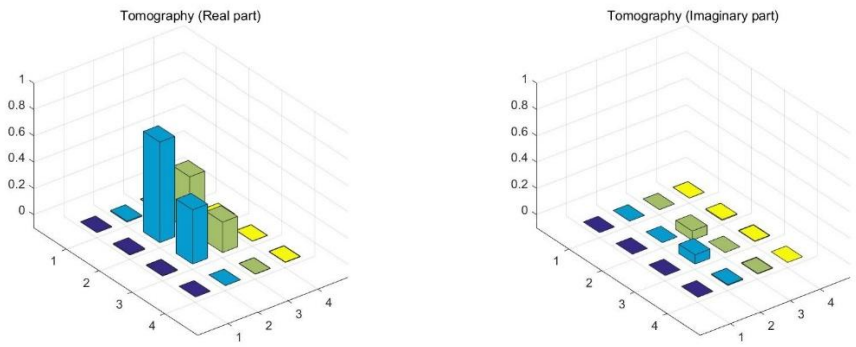

图 1.2 量子态层析结果

设置泵浦光周期为 500kHz，平均每脉冲光子对数为 0.2，纠缠态制备速率为 100kbps。

2. 选基随机序列 X、Y

使用商用量子随机数发生器。

3. 测量模块

3.1 测量基

采用基于普克尔盒（Pockels Cell）的调制技术对单光子进行偏振调制（如图 3.1 所示），透过率优于 99%。Pockels Cell 的半波电压约 2.7KV，采用高压开关对其进行高重频控制。经过调试 Pockels Cell 驱动电压幅度、延迟、宽度等参数后，可得到测量基调制对比度≥99%。在 DIQRNG 中，我们使用选基随机数驱动 Pockels Cell，随机数为 0 时，进行角度为 A1 的测量；随机数为 1 时，Pockels Cell 相当于 45° 半波片，整体光路进行角度为 A2 的测量。

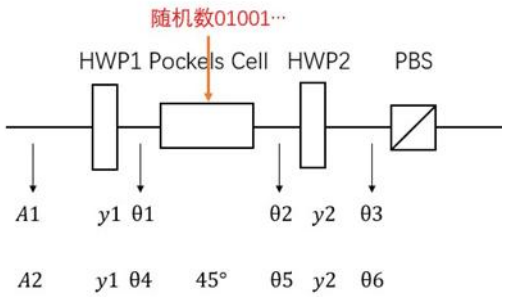

图 3.1 测量基

3.2 探测器

超导纳米线单光子探测器是目前已知的具有高探测效率（如图 3.2），同时满足计数率要求的探测器，测试结果如图 3.3 所示，设置合适的电流值，可使单光子探测效率优于 94%，。

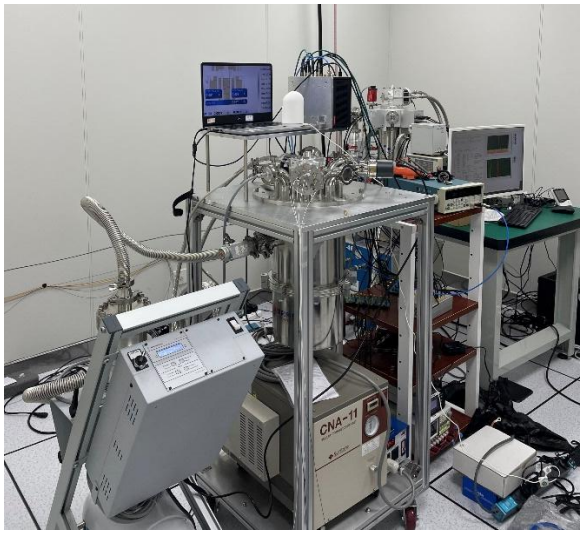

图 3.2 超导纳米线单光子探测器

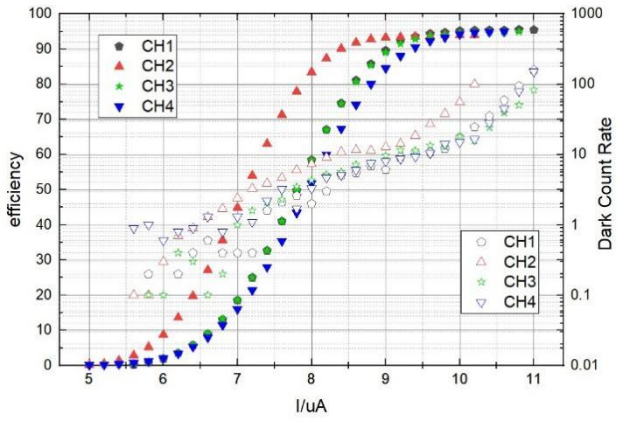

图 3.3 超导纳米线单光子探测器探测效率和暗计数测试结果

4 系统效率

泵浦光为|H⟩时，测得系统效率分别为 86.842%(±0.413%)，87.487%(±0.416%)；泵浦光为|V⟩时，测得系统效率分别为 86.842%(±0.413%)，87.487%(±0.416%)。

5 贝尔检验

数据采集信息如下：

	a=0, b=0	a=0, b=1	a=1, b=0	a=1, b=1
x=0, y=0	23843087	237942	221893	639941
x=0, y=1	23465332	728391	177650	688249
x=1, y=0	23506658	178141	667565	703779
x=1, y=1	22297712	1278495	1233675	131488

可得：

$$S = 0.006 > 0.$$

通过贝尔检验。

6 随机性估计和随机数提取

采用熵累积方法（entropy accumulation theorem, EAT）进行随机性估计，采用 Toeplitz 方法进行随机数提取。采集数据 10 小时，获得 3.1×10^8bits 器件无关量子随机数，随机数产率为 8.6kbps。