ICS 35.040
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

器件无关量子随机数产生器通用要求

General requirements for device-independent quantum random number generators

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

（本草案完成时间：2024 年 5 月 26 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 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：

本文件主要起草人：

器件无关量子随机数产生器通用要求

1 范围

本文件描述了器件无关量子随机数产生器的术语和定义、符号、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。

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 42565-2023 量子计算 术语和定义

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

一类用于检验节点间局域隐变量理论的不等式，也称贝尔型不等式。

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

黑盒子 black box

在使用一个系统时，不关注其内部构造和原理，而只关注其输入和输出的简化模型，也称黑箱。

3.5

纠缠源 entanglement source

所产生的粒子间存在量子纠缠的粒子源。

注：纠缠源具有不同类型，如基于光子、原子等。

3.6

量子态 quantum state

量子系统的状态。

[来源：GB/T 42565-2023，3.1]

3.7

量子态保真度 fidelity of quantum state

量子态的物理实现与理论模型之间接近程度的一种度量。

[来源：GB/T 42565-2023，4.21]

3.8

量子态测量 quantum state measurement

通过对粒子进行测量来得到**量子态**（3.6）信息的操作过程。

[来源：GB/T 42565-2023，3.21，有修改]

3.9

器件无关 device-independent

安全性不依赖于对量子态制备和测量设备的安全假设的性质。

3.10

器件无关量子随机数产生器 device-independent quantum random number generator；DIQRNG

基于量子力学原理可以产生真随机数的器件，且生成的随机数具备**器件无关**（3.9）特性。

3.11

探测漏洞 detection loophole

当整个系统的探测效率低于某一阈值时，探测到的事件的集合不一定能真实反映全部集合的分布，从而导致探测结果不可信，也称探测效率漏洞。

3.12

系统效率 system efficiency（heralding efficiency）

纠缠粒子从纠缠源产生到被探测的效率。

4 符号

下列符号适用于本文件。

X、Y：选基随机序列。

x、y：选基随机数，是选基随机序列的元素。

A、B：测量模块输出的测量结果序列。

a、b：测量模块输出的测量结果，$a,b \in \{0,1\}$，其中，0表示探测器无响应，1表示探测器响应。

i：第i轮实验。

S_i：第i轮的贝尔不等式的值。

N：实验测量轮数。

ε：失败概率。

S：N轮的贝尔不等式的值。

Pr：事件发生的概率。

t：统计涨落相关的参数。

ρ：量子密度算符。

5 器件无关量子随机数产生器结构组成

5.1 基础构架

DIQRNG由纠缠源、两个选基随机序列、两个测量模块、两个测量结果、贝尔检验模块、数据后处理模块组成，随机控制序列为可选模块。两个测量模块分别需要一个输入接口和一个输出接口，数据后处理模块需要一个输入接口和一个输出接口。结构组成示例见图1。当系统工作时，由纠缠源产生量

子纠缠对并分发给测量模块1和2，测量模块1（2）根据选基随机序列X（Y），选择不同的测量基矢对接收到的量子态进行测量，输出测量结果A（B）。将纠缠源和测量模块看作黑盒子，在满足如下假设时，仅根据选基随机序列和测量结果，即可检验器件无关量子随机数的结果是否具有量子随机性：

a）量子力学理论是正确且完备的；

b）选基随机序列是可信的；

c）用于随机性评估和随机性提取的后处理程序是可信的。

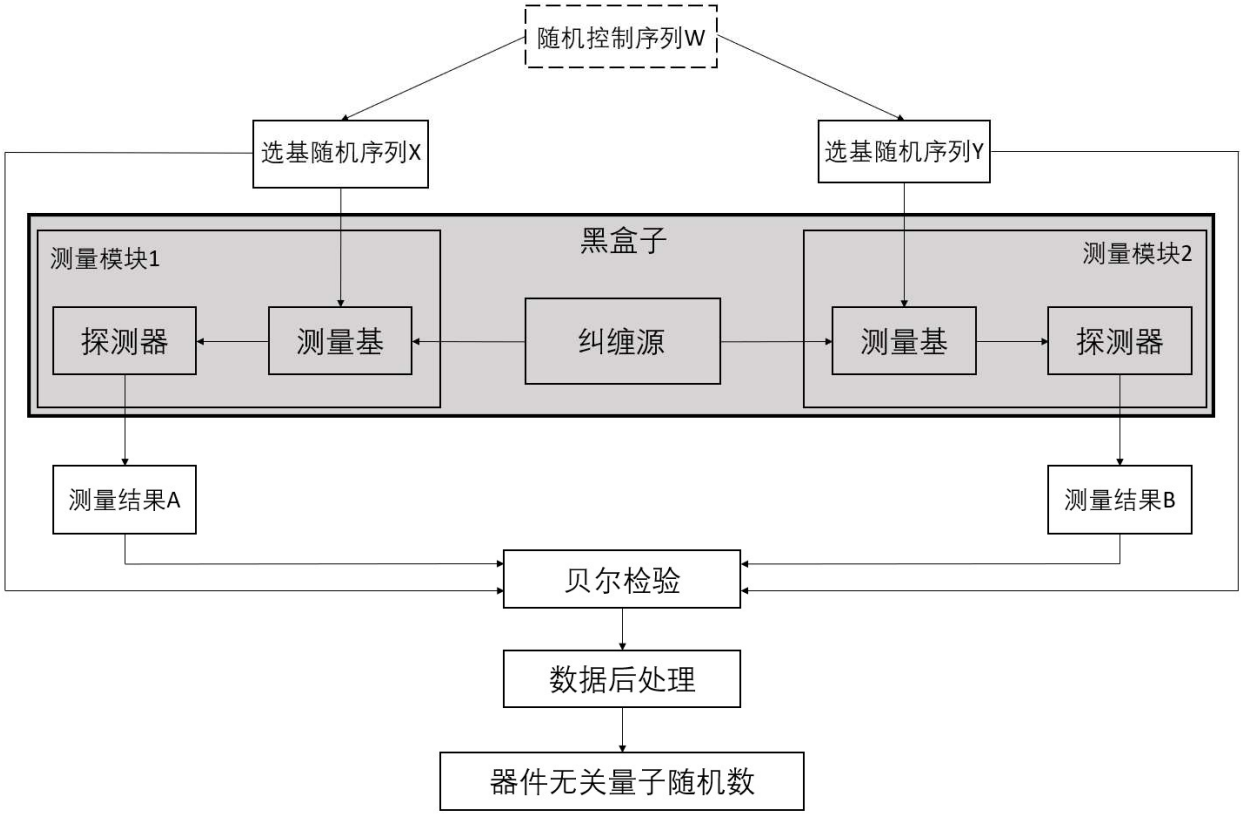

图1　DIQRNG结构组成示例图

5.2 模块功能

5.2.1 纠缠源

纠缠源周期性生成纠缠粒子对，分别分发至测量模块1和测量模块2。

5.2.2 随机控制序列W

随机控制序列W用于随机切换检验轮和生成轮。其中，检验轮进行贝尔检验，同时也可生成随机数，生成轮仅进行随机数生成。因此，此模块为可选模块，当无此模块时，仅存在检验轮。

5.2.3 选基随机序列X、选基随机序列Y

选基随机序列X和Y分别输入测量模块1和测量模块2，用于选择测量基。

注：当存在随机控制序列W时，选基随机序列X和Y仅作用于检验轮。

5.2.4 测量模块

测量模块由测量基和探测器构成。测量基对接收到的纠缠粒子在某个基矢下进行量子态测量。该测量基具备切换功能，可以依据选基随机数x（y）实现不同基矢下的量子态测量，其中x（y）为选基随机序列X（Y）的元素。探测器对纠缠粒子进行探测，并输出信号。

5.2.5 测量结果 A、测量结果 B

测量结果A/B为探测器每个周期的输出结果a/b的统计序列，$a,b \in \{0,1\}$，其中，0表示探测器无响应，1表示探测器响应。

5.2.6 贝尔检验

将检验轮的选基随机序列X和Y、测量结果A和B输入该模块，计算贝尔不等式的值。

5.2.7 数据后处理

如果贝尔不等式的值通过检验，则将贝尔不等式的值、测量结果输入数据后处理模块，进行随机性估计，依据随机性估计结果，将测量结果进行随机数提取，提取的结果为器件无关量子随机数。

6 安全性要求

6.1 模块要求

6.1.1 纠缠源要求

纠缠源应满足以下要求：

a) 纠缠态的制备速率应满足随机数产率的设计需求，本文件建议纠缠态制备速率不低于 50kbps；

b) 纠缠源应具备较高的量子态保真度，本文件建议量子态保真度不低于 90%。

6.1.2 选基随机序列 X/Y 的选基随机序列信息不可泄露。

6.1.3 测量模块的测量效率宜不低于 90%。

6.2 器件无关性

6.2.1 概述

器件无关性检验包括系统效率检验、非信令条件检验、贝尔检验、最小熵评估四个部分。通过系统效率和非信令检验来判断贝尔检验的探测漏洞和局域性漏洞是否被关闭，从而确保器件无关性检验的有效性。

注：自由选择漏洞的关闭由选基随机序列的不可泄露性保证。

6.2.2 系统效率检验

系统效率应大于关闭贝尔检验探测漏洞所需的理论阈值，该阈值由贝尔检验中使用的贝尔不等式决定。如果系统效率低于理论阈值，即使探测到的纠缠粒子能够通过贝尔检验也不能说明检验过程中所有的纠缠粒子能够通过贝尔检验。具体系统效率检验宜根据附录A.1进行计算。

6.2.3 非信令条件检验

为确保两个测量模块的测量行为相互独立，需要以下四组变量满足非信令条件：

a) 测量模块 1 输入的选基随机数x=0 时，其输出测量结果a与测量模块 2 输入的选基随机数y；

b) 测量模块 1 输入的选基随机数x=1 时，其输出测量结果a与测量模块 2 输入的选基随机数y；

c） 测量模块2输入的选基随机数y=0时，其输出测量结果b与测量模块1输入的选基随机数x；

d） 测量模块2输入的选基随机数y=1时，其输出测量结果b与测量模块1输入的选基随机数x。

非信令条件宜根据附录A.1进行计算。

6.2.4 贝尔检验

检验轮的选基随机序列和测量结果应通过贝尔检验。贝尔不等式有多种形式，本文件推荐贝尔不等式如下：

纠缠对分别分发至两个测量模块，根据输入的选基随机数$x,y\in\{0,1\}$的值进行投影测量，测量结果$a,b\in\{0,1\}$。按照公式（1）计算贝尔不等式结果：

$$S_i=\Pr(a_i=0,b_i=0|x_i=0,y_i=0)-\Pr(a_i=0,b_i=1|x_i=0,y_i=1)$$
$$-\Pr(a_i=1,b_i=0|x_i=1,y_i=0)-\Pr(a_i=0,b_i=0|x_i=1,y_i=1)\ )\cdots\cdots(1)$$

式中：

i——表示第i轮实验；

S_i——表示第i轮的贝尔不等式结果；

Pr——表示事件发生的概率。

应使用Hoeffding不等式对贝尔检验进行参数估计，方法如下：通过器件无关量子随机数产生器在N次重复测量后采集的数据，按照公式（2）统计平均贝尔不等式结果：

$$\bar{S}=\frac{1}{N}\sum_{i=1}^{N}S_i\cdots\cdots(2)$$

按照公式（3）估计的贝尔不等式的值：

$$S=\bar{S}-\frac{t}{N}\cdots\cdots(3)$$

式中：

N——实验测量次数，典型值为1×10^8；

t——因统计涨落引入的参数，典型值为1.72×10^4。

如果$S>0$，认为通过贝尔检验。

6.2.5 平滑条件最小熵评估方式

根据器件无关量子随机数产生器的贝尔不等式的值，对测量结果的随机性进行评估。本文件要求随机性以平滑条件最小熵(smooth conditional min-entropy)进行度量。本文件推荐量子概率估计方法，熵累计方法，以及量子互补性方法。本文件推荐的估计方法于附录B给出。这里给出平滑条件最小熵定义。给定两体量子态$\rho_{S_AS_E}$，其中S_A系统对应于器件无关量子随机数产生器进行贝尔不等式的选基随机序列和测量结果，S_E系统对应于可能存在的量子侧信息。在给定的平滑参数$\varepsilon>0$的条件下，S_A系统关于S_E系统在ρ上的ε-平滑条件最小熵由公式（4）给出：

$$H_{\min}^{\varepsilon}(S_A|S_E)_\rho=\max_{P(\rho,\rho')\le\varepsilon}H_{\min}(S_A|S_E)_{\rho'}\cdots\cdots(4)$$

其中ρ'为作用于S_A、S_E联合系统上的次归一化量子密度算符（sub-normalized density operator），$P(\rho,\rho')$为ρ和ρ'间的纯化距离（purified distance），由公式（5）给出：

$$P(\rho,\rho')=\sqrt{1-\left(\mathrm{tr}\left|\sqrt{\rho}\sqrt{\rho'}\right|+\sqrt{[1-\mathrm{tr}(\rho)][1-\mathrm{tr}(\rho')]}\right)^2}\cdots\cdots(5)$$

$H_{\min}(S_A|S_E)_{\rho'}$为$S_A$系统关于$S_E$系统在$\rho'$上的最小熵，由公式（6）给出：

$$H_{\min}(S_A|S_E)_{\rho'}=\sup_{\sigma}\sup_{\lambda}\{\lambda\in\mathbb{R}:\rho'\le\exp(-\lambda)I_A\otimes\sigma\}\cdots\cdots(6)$$

其中，σ为作用于S_E系统上的次归一化量子密度算符。

6.3 数据后处理

数据后处理设计应满足以下要求：

a) 应采用合理的随机性估计方法，可参考附录 B.1；

b) 应采用合理的随机数提取方法，可参考附录 B.2。

检测方法如下：

a) 提供源代码，进行代码走查；

b) 对于支持在线输入的设备，在线输入多种标准输入，比较后处理算法的输出和相应的标准输出，观察是否一致；

c) 对于不支持在线输入的设备，可在模拟器上仿真源代码。审查模拟器代码，保证源代码中关键参数和源代码一致，且可以正确实现所需要的功能；

d) 记录输入的选基随机序列长度，以及后处理算法相应输出的二元随机序列长度。计算出对于每单位长度的随机输入，后处理提取输出的二元随机序列长度，要求该长度不大于熵评估给出的量子随机成分最小熵值。

6.4 随机性检验

最终输出随机数应依据GM/T 0005-2021规定进行随机数检测。第一次检测不合格时，允许重复1次随机数采集与检测，如果重复检测仍不合格，则判定为随机数发生器失效。

附 录 A
（规范性）
器件无关性检测方法和随机数产率测试方法

A.1 器件无关性检验方法

器件无关性检测通过无漏洞贝尔检验来完成，贝尔检验的主要过程如图1所示：纠缠源分发纠缠对至测量模块1和测量模块2，两个模块分别依据选基随机序列X和Y选择测量基对纠缠粒子进行测量，经过探测器探测后给出测量结果A和B。使用 X、Y、A、B计算贝尔不等式的值。在关闭探测效率漏洞和满足非信令条件的情况下，若通过贝尔检验，则证明存在量子随机性，可以用来产生器件无关量子随机数。

关闭探测漏洞的核心指标为系统效率。系统效率测试方法如下：

两个测量模块对纠缠源分发的纠缠对进行测量，使用时间数字转换器进行数据分析，分别得到单路计数率C_1和C_2，以及符合计数率C_{12}。按照公式（A.1）和（A.2）分别计算两个测量模块的系统效率。

$$\eta_1 = \frac{C_{12}}{C_2} \quad \text{(A.1)}$$

$$\eta_2 = \frac{C_{12}}{C_1} \quad \text{(A.2)}$$

式中：

C_1——测量模块1中探测器的单路计数率；

C_2——测量模块2中探测器的单路计数率；

C_{12}——测量模块1和测量模块2中探测器的符合计数率；

η_1——测量模块1的系统效率；

η_2——测量模块2的系统效率。

系统效率均应大于76%。

非信令条件判断方法如下：

将器件无关量子随机数产生器运行一段时间，进行贝尔检验共计N轮次，依据前i-1轮次，得到概率分布F公式（A.3）：

$$\mathrm{F} = \{p_{xy} f(ab|xy), a, b, x, y = 0,1\} \quad \text{(A.3)}$$

式中：

a——测量模块1的测量结果；

b——测量模块2的测量结果；

x ——测量模块1的选基随机数；

y——测量模块2的选基随机数；

p_{xy}——两个测量模块选基随机数的概率分布。

根据公式（A.4）计算满足非信令条件的概率分布$\mathbf{p}_{NS}^{*}$：

$$\mathbf{p}_{NS}^{*} = \{p_{xy} p_{NS}^{*}(ab|xy), a, b, x, y = 0,1\} \quad \text{(A.4)}$$

式中：

$p_{NS}^{*}(ab|xy)$——在不同选基随机数x、y条件下满足非信令条件的测量结果ab的概率分布。

根据公式（A.5）计算Kullback-Leibler(KL)散度。

$$D_{KL}(\mathrm{f}||\mathbf{p}_{NS}) = \sum_{a,b,x,y} p_{xy} f(ab|xy) \log_2 \left(\frac{f(ab|xy)}{p_{NS}(ab|xy)} \right) \quad \text{(A.5)}$$

式中：

$f(ab|xy)$——在选基随机数xy条件下测量结果ab的概率；

$p_{NS}(ab|xy)$——在选基随机数xy条件下满足非信令条件的测量结果ab的概率。

当$D_{KL}(\mathrm{f}||\mathbf{p}_{NS})$最小值时，得到$\mathbf{p}_{NS}^{*}$。

从第i轮开始计算

$$p_n = \min((\prod_{i=1}^{n} R_i(a_i b_i x_i y_i))^{-1}, 1) \quad \text{(A.6)}$$

式中：

$$R(ABXY) = \frac{f(AB|XY)}{p_{NS}^{*}(AB|XY)}$$

如果$p_n = 1$，则证明满足非信令条件。

A.2 随机数产率测试方法

随机数产率测试按照以下步骤进行：

a) 对量子随机性定量估计方案进行原理性审查；

b) 对随机数提取方案进行原理性审查；

c) 对源代码进行代码走查，包括数据采集、数据分析、量子随机性估计及随机数提取；

d) 正确配置器件无关量子随机数产生器，使其正常工作，采集单位时间内输出的全部随机数，依据公式（A.7）和（A.8）的计算方法计算产率和净产率，检查是否满足产品手册中规定的指标要求。

$$G = R/T \quad \text{(A.7)}$$

$$NG = (R - CR_{XY} - CR_{EX})/T \quad \text{(A.8)}$$

式中：

G——随机数产率；

R——采集的随机数总量；

T——采集时间；

NG——随机数净产率；

CR_{XY}——消耗的选基随机数量；

CR_{EX}——随机数提取中消耗的随机数量。

附 录 B
（资料性）
随机性估计方法和随机数提取方法

B.1 随机性估计方法

B.1.1 量子概率估计方法（quantum probability estimation, QPE）

将DIQRNG的检验轮的选基随机序列和测量结果作为训练集，估计该DIQRNG的输出概率分布，优化每轮贝尔检验的量子估计因子（quantum estimation factors, QEF），可得到随机性的期望速率。

具体方法可参见参考文献1。本文件给出推荐估计方法如下：对于推荐使用的贝尔不等式，将贝尔不等式测量中，所有由$\boldsymbol{x},\boldsymbol{y},\boldsymbol{a},\boldsymbol{b}$和可能存在的量子侧信息$\tau_E$构成的联合量子态集合记为$M(\boldsymbol{x},\boldsymbol{y},\boldsymbol{a},\boldsymbol{b})$，优化寻找符合下述条件的量子估计因子$F(\boldsymbol{xyab})$：

$$\sum_{\boldsymbol{x},\boldsymbol{y},\boldsymbol{a},\boldsymbol{b}} F(\boldsymbol{xyab})\,\mathcal{R}_\alpha[\tau_E(\boldsymbol{xyab})|\tau_E(\boldsymbol{xy})] \le 1 \quad \text{(B.1)}$$

式中：

$\boldsymbol{x}$——测量模块1的全部选基随机数；

$\boldsymbol{y}$——测量模块2的全部选基随机数；

$\boldsymbol{a}$——测量模块1的全部测量结果；

$\boldsymbol{b}$——测量模块2的全部测量结果；

α——预先确定的常数，合法取值范围为$\alpha > 1$

$\tau_E(\boldsymbol{xyab})$和$\tau_E(\boldsymbol{xy})$——由公式（B.2）给出：

$$\tau = \sum_{\boldsymbol{x},\boldsymbol{y},\boldsymbol{a},\boldsymbol{b}} |\boldsymbol{xyab}\rangle\langle\boldsymbol{xyab}| \otimes \tau_E(\boldsymbol{xyab})$$

$$\tau_E(\boldsymbol{xy}) = \sum_{\boldsymbol{x},\boldsymbol{y},\boldsymbol{a},\boldsymbol{b}} \tau_E(\boldsymbol{xyab}) \quad \text{(B.2)}$$

$\mathcal{R}_\alpha$——α阶Rényi幂次，由公式（B.3）给出：

$$\mathcal{R}_\alpha(\rho|\sigma) = \mathrm{tr}\left[\left(\sigma^{-\frac{\alpha-1}{2\alpha}}\rho\sigma^{-\frac{\alpha-1}{2\alpha}}\right)^\alpha\right] \quad \text{(B.3)}$$

α可以预先进行优化选取。按照QPE理论，给定平滑参数$\varepsilon \in (0,1)$，当DIQRNG原始测量结果对应的QEF满足（B.4）：

$$F(\boldsymbol{xyab}) \ge 2^{h(\alpha-1)} \quad \text{(B.4)}$$

式中：

h——设计的DIQRNG随机数产生数量阈值

所得到的ε-平滑最小熵估计结果为：

$$H_{\min}^{\varepsilon}(\boldsymbol{AB}|\boldsymbol{XY}S_E)_\tau \ge h - \frac{1}{\alpha-1}\log_2\left(\frac{2}{\varepsilon^2}\right) + \frac{\alpha}{\alpha-1}\log_2\kappa \quad \text{(B.5)}$$

式中：

κ——设计的DIQRNG正常运行的概率，推荐取值$\kappa = \varepsilon$；

$\boldsymbol{X}$——测量模块1的选机随机序列；

$\boldsymbol{Y}$——测量模块2的选机随机序列；

$\boldsymbol{A}$——测量模块1的测量结果随机序列；

$\boldsymbol{B}$——测量模块2的测量结果随机序列；

S_E——DIQRNG潜在的量子侧信息对应的系统。

B.1.2 熵累积方法（entropy accumulation theorem, EAT）

熵累积方法可通过DIQRNG贝尔检验结果，得到可提取的随机性下限。具体方法可参见参考文献2。本文件给出推荐估计方法如下：对于推荐使用的贝尔不等式，在给定平滑最小熵参数$\varepsilon \in (0,1)$下，ε-平滑条件最小熵由下述公式组（B.6）-（B.11）给出：

$$H_{\min}^{\varepsilon}(\boldsymbol{AB}|\boldsymbol{XY}S_E) \geq NR_{\mathrm{opt}}(\varepsilon,\varepsilon_{EA}) \cdots\cdots (B.6)$$

式中：

$\boldsymbol{X}$——测量模块1的选机随机序列；

$\boldsymbol{Y}$——测量模块2的选机随机序列；

$\boldsymbol{A}$——测量模块1的测量结果序列；

$\boldsymbol{B}$——测量模块2的测量结果序列；

S_E——DIQRNG潜在的量子侧信息对应的系统；

N——实验测量次数；

ε_{EA}——预先设定的EAT参数，合法取值范围为$(0,1)$；

$R_{\mathrm{opt}}(\varepsilon,\varepsilon_{EA})$——按照（B.7）计算：

$$R_{\mathrm{opt}}(\varepsilon,\varepsilon_{EA}) = \max_{\frac{3}{4}<p_t<\frac{2+\sqrt{2}}{4}} R(\omega,p_t,\varepsilon,\varepsilon_{EA}) \cdots\cdots (B.7)$$

式中：

p_t——可以优化选取的参数，取值范围为$p_t \in \left(\frac{3}{4},\frac{2+\sqrt{2}}{4}\right)$；

ω由公式（B.8）给出：

$$\omega = \frac{S}{2}+\frac{3}{4} \cdots\cdots (B.8)$$

其中，S为按照6.2.4节要求的方式进行估计得到的贝尔不等式的值；

$$R(p,p_t,\varepsilon,\varepsilon_{EA}) = f_{\min}(p,p_t) - \frac{1}{\sqrt{n}}2\left(\log_2 13 + \frac{\mathrm{d}}{\mathrm{d}p}g(p)|_{p_t}\right)\sqrt{1-2\log_2(\varepsilon\varepsilon_{EA})} \cdots\cdots (B.9)$$

式中：

$\frac{\mathrm{d}}{\mathrm{d}p}g(p)|_{p_t}$为公式（B.10）、（B.11）在$p=p_t$处的导数：

$$g(p) = \begin{cases} 1-h\left(\frac{1}{2}+\frac{1}{2}\sqrt{16p(p-1)+3}\right), p \in \left[0,\frac{2+\sqrt{2}}{4}\right] \\ 1, \frac{p}{q} \in \left(\frac{2+\sqrt{2}}{4},1\right] \end{cases} \cdots\cdots (B.10)$$

$$f_{\min}(p,p_t) = \begin{cases} g(p), p \leq p_t \\ \frac{\mathrm{d}}{\mathrm{d}p}g(p)|_{p_t}p + \left[g(p_t) - \frac{\mathrm{d}}{\mathrm{d}p}g(p)|_{p_t}p_t\right], p > p_t \end{cases} \cdots\cdots (B.11)$$

B.1.3 量子互补性方法（quantum complementarity approach）

量子互补性方法可通过DIQRNG贝尔检验结果，得到可提取的随机性下限。具体方法可参见参考文献3。本文件给出推荐估计方法如下：给定平滑最小熵参数$\varepsilon \in (0,1)$,在满足公式（B.12）的条件下：

$$\varepsilon = \sqrt{2(\varepsilon_{pc}+\varepsilon_{pe})} \cdots\cdots (B.12)$$

式中：

ε_{pe}——预先设定的相位错误（phase error）估计参数，合法取值范围为$(0,1)$；

ε_{pc}——预先设定的相位错误纠正参数，合法取值范围为$(0,1)$；

ε-平滑条件最小熵由公式（B.13）计算：

$$H_{\min}^{\varepsilon}(\boldsymbol{AB}|\boldsymbol{XY}S_E) \geq N\left[1 - I\left(\omega, \varepsilon_{pe}\right)\right] - \log_2 \varepsilon_{pc} \quad \text{(B.13)}$$

式中$I\left(\omega, \varepsilon_{pe}\right)$由公式（B.14）计算：

$$I\left(\omega, \varepsilon_{pe}\right) = \min_{\xi \in \left(0, \frac{1}{2}\right)} \left\{ h\left[e_p^{\xi}(\omega)\right] + \log_2\left(\frac{1+2\xi}{\xi}\right) \sqrt{-\frac{\ln \varepsilon_{pe}}{2n}} \right\} \quad \text{(B.14)}$$

式中：

$\boldsymbol{X}$——测量模块1的选机随机序列；

$\boldsymbol{Y}$——测量模块2的选机随机序列；

$\boldsymbol{A}$——测量模块1的测量结果序列；

$\boldsymbol{B}$——测量模块2的测量结果序列；

S_E——DIQRNG潜在的量子侧信息对应的系统；

N——实验测量次数；

h——由下述公式给出的函数：

$$h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$$

ξ——可以优化选取的参数，取值范围为$\xi \in \left(0, \frac{1}{2}\right)$；

$e_p^{\xi}(\omega)$——由公式（B.15）、（B.16）计算：

$$e_p^{\xi}(\omega) = \begin{cases} \frac{1+2\xi-\sqrt{\left(\frac{\omega}{2}\right)^2-1}}{2(1+2\xi)}, 2 < \omega \leq 2\sqrt{2} \\ \frac{1}{2}, 0 \leq \omega \leq 2 \end{cases} \quad \text{(B.15)}$$

$$\omega = 4S + 2 \quad \text{(B.16)}$$

S为按照6.2.4节要求的方式进行估计得到的贝尔不等式的值。

B.2 随机数提取方法

B.2.1 Trevisan 提取

Trevisan 提取算法是抗量子强提取算法。将随机数种子进行分组后与DIQRNG的测量结果输入至一比特随机数提取器中，通过级联一比特随机数提取器的输出，得到提取后的随机数。

B.2.2 Toeplitz 提取

Toeplitz 提取算法是抗量子强提取算法。m×n Toeplitz 矩阵的元素均为二进制随机比特，结构见公式（B.17）：

$$T_{m\times n} = \begin{pmatrix} a_0 & a_{-1} & \cdots & a_{-(n-2)} & a_{-(n-1)} \\ a_1 & a_0 & \ddots & & a_{-(n-1)+1} \\ a_2 & a_1 & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & a_{-(n-1)+(m-2)} \\ a_{m-1} & a_{m-2} & \cdots & a_{-n+(m-1)} & a_{-(n-1)+(m-1)} \end{pmatrix} \quad \text{(B.17)}$$

DIQRNG 的测量结果可组成矩阵公式（B.18）：

$$D_n = \begin{pmatrix} d_1 \\ d_2 \\ \cdots \\ d_{n-1} \\ d_n \end{pmatrix} \quad \text{(B.18)}$$

提取后的随机数矩阵可按照公式（B.19）计算：

$$R_m = T_{m\times n} \cdot D_n \quad \text{(B.19)}$$

参 考 文 献

[1]Y. Zhang, H. Fu, and E. Knill, Phys. Rev. Research 2, 013016 (2020).

[2]Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. Commun. Math. Phys. 379, 867–913 (2020); Dupuis, F. & Fawzi, O. Entropy accumulation with improved second-order term. IEEE Trans. Inf. Teory 65, 7596–7612 (2019).

[3]Zhang, X., Zeng, P., Ye, T., Lo, H. K., & Ma, X. Quantum complementarity approach to device-independent security. Phys. Rev. Lett., 131(14), 140801 (2023).