随机数发生器
QRNG 系列
产品白皮书

上海循态量子科技有限公司

本文档的全部内容属于上海循态量子科技有限公司所有，未经明确书面许可，任何单位或个人不可擅自引用、复制、誊抄或转译本文档部分或全部内容，不得以任何形式或方式（电子、机械、影印、录制或其它可能的方式）进行商业传播或用于任何商业、盈利目的。

1. 引言

1.1. 随机数

随机数是专门的随机试验的结果。在统计学的不同技术中需要使用随机数，比如在从统计总体中抽取有代表性的样本的时候，或者在将实验动物分配到不同的试验组的过程中，或者在进行蒙特卡罗模拟法计算的时候等等。

产生随机数有多种不同的方法。这些方法被称为随机数发生器。随机数最重要的特性是：它所产生的后面的那个数与前面的那个数毫无关系。

随机数在密码学中非常重要，保密通信中大量运用的会话密钥的生成即需要真随机数的参与。如果一个随机数生成算法是有缺陷的，那么会话密钥可以直接被推算出来。若果真发生这种事故，那么任何加密算法都失去了意义。

1.2. 伪随机数

伪随机数（PRNG）是通过数学的方法由计算机产生的，现代计算机算法已经可以产生足够好的伪随机数，伪随机数虽然快捷，但是它产生的随机数是先定的，对于同样的种子，产生的随机序列将会是相同的，所以在加密应用中，如果攻击者拥有足够的计算能力，则可以对伪随机数加密进行破解。

一般地，伪随机数的生成方法主要有以下 3 种：

（1） 直接法（Direct Method），根据分布函数的物理意义生成。缺点是仅适用于某些具有特殊分布的随机数，如二项式分布、泊松分布。

（2） 逆转法（Inversion Method），假设 U 服从[0，1]区间上的均匀分布，令 X=F-1（U），则 X 的累计分布函数（CDF）为 F。该方法原理简单、编程方便、适用性广。

（3）接受拒绝法（Acceptance-Rejection Method）：假设希望生成的随机数的概率密度函数（PDF）为 f，则首先找到一个 PDF 为 g 的随机数发生器与常数 c，使得 f（x）≤cg（x），然后根据接收拒绝算法求解。由于算法平均运算 c 次才能得到一个希望生成的随机数，因此 c 的取值必须尽可能小。显然，该算法的缺点是较难确定 g 与 c。

因此，伪随机数生成器（PRNG）一般采用逆转法，其基础是均匀分布，均匀分布 PRNG 的优劣决定了整个随机数体系的优劣。

真正的随机数是使用物理现象产生的：比如掷钱币、骰子、转轮、使用电子元件的噪音、核裂变等等，这样的随机数发生器叫做物理性随机数发生器，它们的缺点是技术要求比较高。

基于随机性的来源定义随机数是量子随机数发生器还是伪随机数发生器。

特征	伪随机数序列	热噪声随机数	量子随机数序列
产生方法	确定性算法	用带有抖动的低频振荡器通过触发器采样有固定周期的高频振荡器	量子随机性现象的采样
产生效率	极高效率	≤20Mbps	500Mbps~10Gbps
周期性	周期性	非周期性	非周期性
可预测性	可能被预测	不可被预测	不可被预测
可重复性	可能被复制	可能被复制	不可能被复制

1.3. 量子随机数

长期以来,随机数的产生是统计学、信息学以及密码学研究的焦点之一。高质量的真随机数有助于统计学中对规律现象的建模和评估，同时在数值计算方法和数学模拟中（例如 Monte Carlo），以及在博彩业（如彩票，博弈），随机码验证，随机检验等方面有着重要的应用。随机数在密码学中的应用非常普遍,例如经典密码算法中的密钥生成和分配，以及当前量子信息领域的研究热点——量子密钥分发系统中量子态的制备和测量都需要使用随机数。随机数的质量在很大程度上影响着这些加密算法或协议的安全性。

传统的随机数发生器大多基于复杂的数学算法和经典物理过程，是伪随机数，而不是真随机数。真随机数序列具有均匀无周期性，不可预测性和不可重复性。真随机数序列的产生依赖于对物理现象的测量、采样以及算法后处理来实现。并

且真随机只有在量子世界中存在，所以利用具有量子特性的物理源来产生纯净的真随机数序列的随机数设备称之为量子真随机数发生器，量子随机数发生器是迄今为止唯一的从理论上可以论证的真正的随机数发生器，其本质是由量子力学的基本原理决定的。

1.4. 量子随机数国内外发展现状

目前，量子随机数生成技术的发展方向主要是集中在提高量子随机数的生成速度，缩小量子随机数发生器件的尺寸，以及降低量子随机数发生器的成本上。密码学的很多场景对于真随机数的产生速度有着很高的需求。比如在量子通信中，新一代的量子通信设备的工作频率（每秒钟发送的量子信号数量）逐步提升到 GHz，而在编解码过程中，量子通信需要使用数倍甚至更多的真随机数进行编码和解码。因此，量子通信系统，对于真随机数生成速度的需求提升到了 10Gbps 甚至更高。

循态量子

2. 产品介绍

2.1. 产品简介

上海循态量子科技有限公司 2020 年发布了实现基于量子真空态涨落测量机理的商业化量子真随机发生器 QRNG-102（如下图所示），该款产品是 PCIe 接口、全高半长尺寸、最终的随机数生成速率可达 2Gbps 达到国内外在同等速率下尺寸最小，应用于区块链，物联网、科学仿真等领域，取得良好的客户反响。

QRNG-102 产品图

上海循态量子科技有限公司在 2021 年发布了基于真空涨落噪声机理的商业化量子随机数发生器 QRNG-200（如下图所示），该款产品的外部接口形态是 PCIe3.0×4、半高半长尺寸、最终的随机数生成速率为 10Gbps，是目前全球速率最高的商业化量子随机数产品。

QRNG-200 产品图

循态量子

2.2. 产品特点

- 系统状态实时监控
- 量子真随机数源
- 经济、紧凑、可靠性高
- 可操作性、扩展性强
- 兼容各种主流操作系统
- 提供友好图形界面交互功能
- 稳定性高，对环境的扰动不敏感
- 开放标准API接口库，方便二次开发

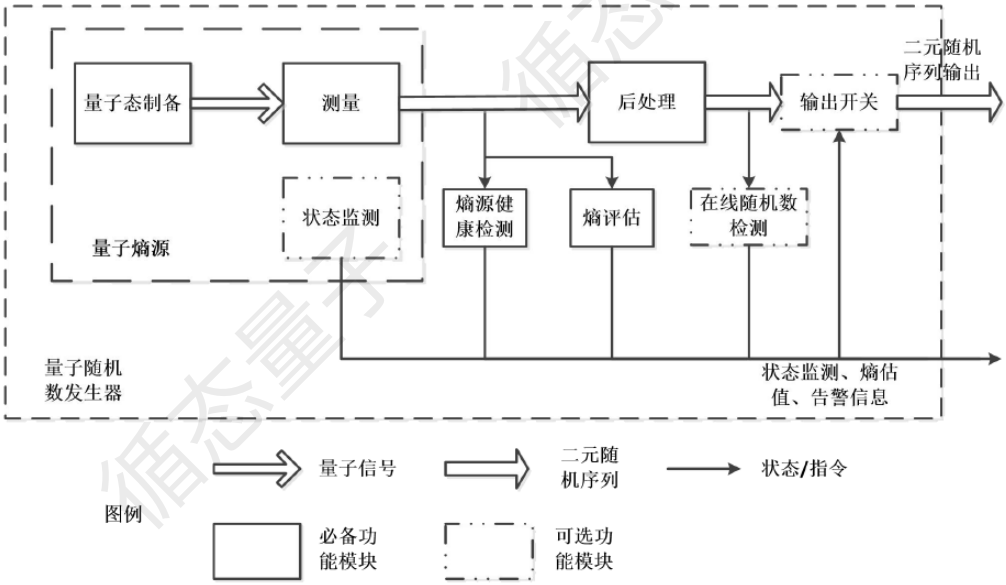
2.3. 产品参数

产品型号	QRNG-100	QRNG-101	QRNG-102	QRNG-200	QRNG-201
实时生成速率	256Mbps	512Mbps	1Gbps	4Gbps	10Gbps
接口	PCIE2.0 X4			PCIE3.0 X4	
尺寸（最大）	180.75*126.29*22.05mm			181.30*80.20*24.58mm	
外观	标准全高半长 PCIe 卡			标准半高半长 PCIe 卡	
工作温度	-20~40°C			-10~40°C	
存储温度	-40~85°C			-40~85°C	
湿度	5%~95%			5%~95%	
风扇	≥200LFM			≥200LFM	

循态量子

3. 技术原理

3.1. 总体架构

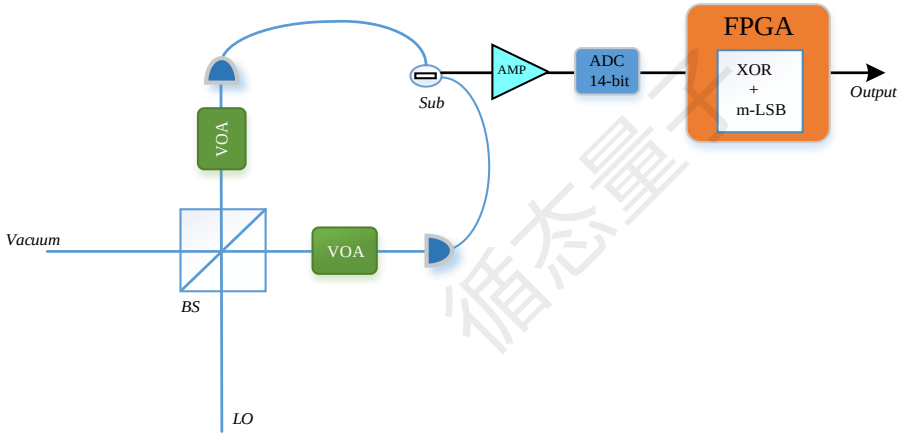


- 量子随机数源模块
- 探测和采样模块
- 算法后处理模块
- 随机性检测模块

3.2. 随机数生成机制

QRNG-102 是基于真空态测量原理的量子随机数发生器，原理如下图所示，QRNG-102 由零差探测模块（包括激光器、光分束器、可调光衰减器、光电探测器）、放大器、模数转换器、熵评估模块、后处理模块组成。零差探测模块实现对真空态的测量，其中激光器输出连续且稳定的激光作为本地振荡器与真空态相干干涉；光分束将激光器输出的光一分为二；可调光衰减器对分束后的光进行光强调节从而控制零差探测模块的平衡状态；光电探测器将光信号转换为电信号。放大器实现对电信号的放大。模数转换器将模拟电信号转换为数字电信号，转换后的数字信号即量子随机数发生器输出的原始数据。熵评估模块实现对量子熵的

评估。后处理模块利用 FPGA 芯片实现原始数据的预处理与 m-LSB 算法。



基于真空态的 QRNG 方案原理图

QRNG-102 软件实现包括熵评估模块、后处理模块两部分。

熵评估模块实现对原始数据（模数转换器之后、预处理前的数据）量子熵的测量。

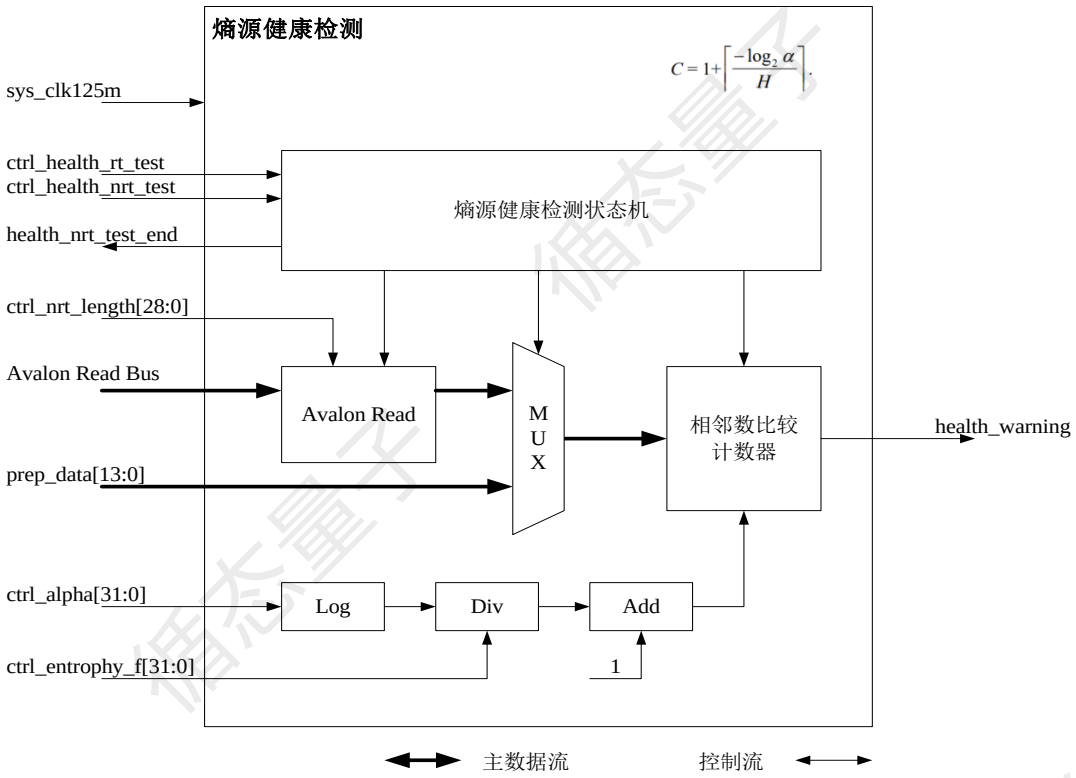
后处理模块包括预处理与 m-LSB 算法。

QRNG-102 先通过数据预处理算法解决数据本身存在的偏置和不对称问题。由于光电探测器、跨阻放大器等器件受电流或温度等参量的影响，经过 ADC 采样的原始序列经常会被一个慢变的包络所调制，它使采样的数据产生较明显的偏置以及使数据统计直方图（histogram）不对称。

QRNG-102 处于正常运行状态下（激光器打开）获取原始数据，原始数据进行数据预处理，计算预处理后数据的方差得到预处理后的经典电噪声的方差，即当 QRNG-102 激光器处于关闭状态时获取经典电噪声，电噪声数据进行数据预处理。

对预处理后数据采用 m-LSB 方法实现对量子真随机性的提取。依据上述熵评估的值，估算出每个预处理后数据（14 位数据）应保留的比特位数 m。

3.3. 熵源健康检测机制



熵源健康检测模块实现框图

熵源健康检测模块通过检测量子熵源输出的原始数据（模数转换器之后、预处理前的数据）来判断熵源的健康与否。如果检出熵源异常，则输出告警脉冲，量子随机数发生器停止输出随机数。

熵源健康检测有两种模式：实时检测模式和非实时检测模式（半小时做一次）。每出现连续 C（$C = \left\lceil 1 + \frac{-\log_2 \alpha}{\mathrm{H}_{min}} \right\rceil$）个相同数据，就输出一个告警脉冲，随机数发生器停止输出随机数。实时检测模式下，H_{min}值是当前一次熵评估的结果，非实时检测模式（半小时做一次）下，H_{min}值是最近熵评估的结果。QRNG-102 的熵源健康检测模式可配置。

4. 应用场景

4.1. 密码学

密码的安全性完全依赖于随机数序列的生成效率和质量。现在的密码系统中大多数仍然利用数学算法或经典物理噪声的方式来产生随机数，经典物理过程在考虑到所有变量的情况下，是可以被模拟和预测的，这样密码系统存在很大的风险。

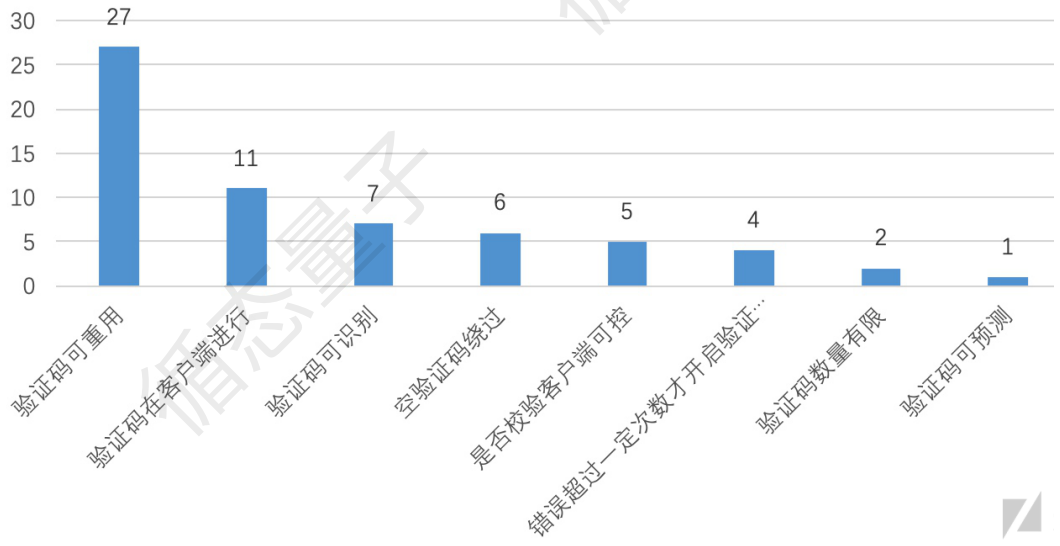
量子真随机数具有分布均匀、无周期性、不可预测、不可重复等特点，可以将量子随机数作用于：

- 密码算法
- 安全认证
- 密码芯片的安全
- 数字签名（数字水印）

循态量子

4.2. 移动端

近年来移动支付为公众带来便利性的同时，也带来一定的风险性。比如对短信验证码的过度信任，是一个值得注意的隐患。短信验证码的安全性级别相对较低，不法分子通过盗窃手机卡、拦截短信、武力胁迫等手段，都可能获取相关短信验证码。如今，每天全球约有 30 亿次的验证点击。



量子真随机数可广泛应用于以下场景的等：

- 短信验证码（身份验证）

  市场规模呈逐年稳定增长态势。2022年我国短信验证码服务规模将达82.8亿元

- 互联网验证码（操作验证码）

  防止恶意批量注册、恶意破解密码、刷票、论坛灌水，以及有效防止黑客对某一个特定注册用户账户暴力破解，同时防止黑客对网站的恶意访问。

4.3. 金融

金融业信息化程度不断提高，对金融业改革、发展、壮大发挥了重要的促进作用。同时，金融业对信息技术的依赖程度越来越大，信息安全保障工作的难度

不断加大，互联网应用又进一步加大了信息安全风险的扩散效应。

在历经了网络建设、数据大集中、网络安全基础设施建设等阶段后，如今，我国金融信息化已进入了体系化信息安全管理的阶段，亟待建立一套金融信息安全保障体系，有效地防范和化解安全风险，统一安全问题处理规范和流程，增强金融系统的信息安全整体防范能力，以保证金融机构的信息系统平稳运行及各项业务的持续展开。

量子随机数可用于取代传统密码熵源，在无需改动原业务框架的基础上极大地增加金融信息的安全性。

- 存储数据加密

  为了防止黑客或内部高权限用户整体拖库，造成大批量明文数据泄露，需对数据库中存储的敏感数据进行加密。通过多级权限控制体系，按角色、IP地址、时间范围对密文进行访问控制，并通过对应用程序或系统进行摘要值和连接随机种子的判定，保证应用身份标识不可伪造，合法连接不可重放，实现数据被盗后无法查看明文的目的。

- 通信数据加密

  银行和金融机构需要确保银行交易和应用程序数据的实时可用性，同时保护敏感的客户和专有信息。

循态量子

4.4. 物联网

物联网安全是指保护连接到无线网络或互联网的物联网设备或支持互联网的设备。物联网安全需要安全地连接物联网设备及其组件，并保护这些设备免受网络攻击。

物联网安全专注于保护设备、它们的网络以及它们所产生的数据。这可以包括个人电脑、笔记本电脑、智能手机、平板电脑、智能家电等。

物联网设备需要收集和传输大量敏感信息，数字识别和使用安全算法来生成密钥来加密客户的数据。传输的数据通常受加密算法保护，使用随机数进行加密。

量子随机数可用于取代传统密码熵源，在无需改动原业务框架的基础上极大地增加物联网信息的安全性。

4.5. 数据中心

为了防止数据丢失，所有企业的数字资产都备份在远程数据中心，保护传输中数据的唯一有效方法是通过数据加密。

循态量子

同时存储在本地的数据加密也不可忽视，勒索攻击事件频发，其攻击规模和频率以惊人的速度增长。预测到 2025 年，75%的企业将面临一次或多次的勒索攻击。随着勒索组织的目标越来越有针对性，以及勒索攻击手段愈演愈烈，勒索攻击已成为国家、企业和个人数据安全的头号公敌。

量子随机数可以和数据中心存储设备深度融合，从多个方面，全链路式的对数据的安全性进行保护。

通过在中心机房部署量子安全加密平台，教育相关的核心数据，通过量子加密设备加密后存储在磁盘阵列。如果需要对数据进行读取或者使用，通过另外一台量子安全解密平台，对数据进行解密使用。

当服务器向存储设备写数据时，经安全平台处理后，数据以密文形态写入存储设备；当服务器向存储设备发出读数据指令时，经安全平台处理后，数据将以明文形态呈现给服务器和终端用户。

安全平台以透明方式工作，其在拓扑中的介入不影响两端设备的配置和使用，用户不会察觉到该设备的存在。

循态量子

4.6. 游戏博彩

在线游戏和彩票需要提供出色的随机性，以确保客户的交易安全及公平性保证。2018 年 8 月，曾火爆一时的 Fomo3D 游戏，就被黑客利用其随机数漏洞，在游戏中获得了巨额的利益。

继 Fomo3D 之后，EOS 上的众多热门 DAPP，尤其是竞猜类游戏，如 Lucky Nuts、EOS.WIN、EOSDice 等，也先后因随机数生成的缺陷遭到了黑客攻击。

循态量子

5. 产品资质

★产品通过上海市软件评测中心的成果鉴定
★产品通过中国信息通信研究院泰尔实验室的产品检测
符合《GB/T 32915-2016 信息安全技术 二元序列随机性检测方法》

5.1. 上海市软件评测中心

报告编号：RT20201224

测 试 报 告

Testing Report

测试类型：成 果 鉴 定 测 试

软件名称：循态随机数检测软件[简称：随机数检测软件]

版 本 号：V1.0

送测单位：上海循态信息科技有限公司

报告日期：二〇二〇年七月二十日

项 目 号：T20201224

上海市软件评测中心有限公司

Shanghai Software Testing Center Co., Ltd.

循态量子

测试结论

受上海循态信息科技有限公司委托，上海市软件评测中心有限公司（SHSTC）于二〇二〇年七月一日至二〇二〇年七月二十日，按照GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则、《SHSTC软件检测规范》的要求，对该单位开发的 “循态随机数检测软件[简称：随机数检测软件] V1.0”进行了成果鉴定测试，测试结论如下：

1) 该软件提供随机数据源。

2) 功能性：

该软件主要由读取size个char的随机数到buffer中、设备重置、获取挂载的随机数生成器板卡数、读取一个short类型的随机数、读取一个int类型的随机数、读取一个float类型的随机数、读取一个double类型的随机数、读取一个大于min和小于max的int类型的随机数等功能模块组成；

该软件实现了循态随机数检测软件操作手册的功能要求；

该软件共有8个功能，通过8个功能，通过率为100%。

3) 易用性：

可辨识性：在借助用户文档集后，能正确理解所有的功能；用户文档集覆盖所有的功能；软件出错消息能被正确地理解。

易学性：在借助用户文档集后，能正确地使用所有的功能。

易操作性：用户界面组成一致。

4) 可靠性

成熟性：测试过程中无异常情况。

容错性：测试过程中，没有软件产品引起整个运行环境死机的情况。

5) 信息安全性

保密性：采用杀毒软件对被测软件进行扫描，检测软件不含有已知的病毒。（杀毒软件：360杀毒软件 5.0.0.8160；病毒库：2020-07-01）。

6) 维护性

易分析性：软件出错时会产生相应的提示信息，可根据提示信息进行诊断产生出错的原因。

7) 可移植性：

适应性：软件能够适应以下软硬件环境。（操作系统：CentOS 3.10）。

8) 用户文档集

完备性：文档集中包含了功能操作说明，文档内容完整。

正确性：文档内容正确、不存在歧义。

一致性：文档内容与软件、各文档之间基本一致。

易理解性：文档使用简体中文，描述易理解。

测试结果：**通过。**

上海市软件评测中心有限公司

二〇二〇年七月二十日

5.2. 中国信息通信研究院泰尔实验室的产品检测

报告编号：B21X72437

检 测 报 告

产 品 名 称	量子随机数发生器
产 品 型 号	XT-QRNG102
委 托 单 位	上海循态信息科技有限公司
生 产 单 位	上海循态信息科技有限公司
检 测 类 别	委托检测

中 国 泰 尔 实 验 室

循态量子

中国泰尔实验室
检测报告

产品名称	量子随机数发生器	产品型号/规格	XT-QRNG102
委托单位	上海循态信息科技有限公司	出厂编号/生产日期	2021 年 5 月 18 日
生产单位	上海循态信息科技有限公司	送样日期	2021 年 6 月 24 日
送样地点	中国泰尔实验室(北京市西城区新街口外大街 28 号)	送样者	周颖明
样品数量	1 个		
检测类别	委托检测	检测项目	6 项
样品初始状态	样品初始状态完好，符合检测要求		
检测依据	GB/T 32915-2016《信息安全技术 二元序列随机性检测方法》		
检测结论	该公司送检的 XT-QRNG102 型量子随机数发生器，经检测，各项性能及技术指标结果如下： 所检性能及技术指标共 6 项，其中量子随机数发生器/[illegible]和量子随机数发生器速率为实测值，其余项均达到 GB/T 32915-2016《信息安全技术 二元序列随机性检测方法》及厂家提供的技术要求中有关规定的要求。 (检验检测专用章) 签发日期：2021 年 6 月 30 日		
备注	本报告部分检测结果按厂家提供的技术要求进行判定。		

批准：　　审核：　　主检：

检 测 结 果

序号	检测项目	单位	标准要求	检 测 结 果	结 论
1	量子随机数发生器尺寸	mm	——	180.5(长)×126.3(宽)×21.4(高)	实测值
2	量子随机数发生器随机性	--	应满足 GB/T 32915-2016 中规定的随机性要求	符合要求	合 格
3	量子随机数发生器速率	bit/s	——	1.03×10^{9}	实测值
4	兼容性	--	上位机软件可在 Windows，Linux 系统上运行	符合要求	合 格
5	温度性能	--	操作温度：0℃～+40℃，各温度点保持 1h 后开机可稳定运行	符合要求	合 格
6	稳定性	--	可连续 24h 稳定运行	符合要求	合 格

以下空白

循态量子