

中华人民共和国通信行业标准

YD/T XXXX.3—XXXX

基于 BB84 协议的量子密钥分发 (QKD)
用关键器件和模块 第 3 部分: 量子随机数
发生器 (QRNG)

Key components and modules for Quantum Key Distribution (QKD) based on BB84
protocol - part 3: Quantum Random Number Generator (QRNG)

(报批稿)

XXXX - XX - XX 发布

XXXX - XX - XX 实施

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 符号和缩略语	1
4 量子随机数发生器结构	2
5 量子随机数发生器的功能模块	3
5.1 量子熵源	3
5.2 熵评估	3
5.3 熵源健康检测	4
5.4 后处理	4
5.5 在线随机性检测	4
6 量子随机数发生器应用接口	5
7 量子随机数发生器测试要求及方法	5
7.1 量子随机数发生器原理审查	5
7.2 量子熵源模块测试	5
7.3 熵源健康检测模块测试	6
7.4 后处理模块测试	6
7.5 随机性检测	7
7.6 应用接口测试要求及方法	7
附 录 A（资料性附录）量子随机数发生器方案原理	8
附 录 B（资料性附录）推荐的熵源健康检测方法	13
附 录 C（资料性附录）后处理方法	15

前 言

YD/T XXXX《基于BB84协议的量子密钥分发（QKD）用关键器件和模块》拟分为以下三个部分：

—第1部分：光源；

—第2部分：单光子探测器；

—第3部分：量子随机数发生器（QRNG）。

本部分是YD/T XXXX的第3部分。

本部分按照GB/T 1.1-2009给出的规则起草。

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这些专利的责任。

本部分由中国通信标准化协会提出并归口。

本部分起草单位：科大国盾量子技术股份有限公司、中国信息通信研究院、中国电子科技网络信息安全有限公司、国科量子通信网络有限公司、华为技术有限公司、中兴通讯股份有限公司、北京邮电大学、山东量子科学技术研究院有限公司、浙江九州量子信息技术股份有限公司、济南量子技术研究院。

本部分主要起草人：赵梅生、贾云、赵文玉、赖俊森、徐兵杰、马彰超、李政宇、徐继东、赵永利、郁小松、武宏宇、宋萧天、周飞、李明翰。

行业标准信息服务平台