ICS 35.030
L 80

中华人民共和国密码行业标准

GM/T 0114—2021

诱骗态 BB84 量子密钥分配产品检测规范

Decoy-state BB84 quantum key distribution product test specification

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件依据 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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：安徽问天量子科技股份有限公司、国家密码管理局商用密码检测中心、中国科学技术大学、中国人民解放军信息工程大学、江苏亨通问天量子信息研究院有限公司、中国电子科技集团第三十研究所、科大国盾量子技术股份有限公司、重庆大学、北京邮电大学、兴唐通信科技有限公司。

本文件主要起草人：刘婧婧、韩正甫、刘云、宋晨、邓开勇、雷银花、徐锦丽、吕春梅、苗春华、刘杰杰、张启发、凌杰、宋欢欢、银振强、陈巍、李宏伟、赵良圆、徐兵杰、何远杭、赵梅生、唐世彪、向宏、蔡斌、喻松、张一辰、于宗文、李申。

诱骗态 BB84 量子密钥分配产品检测规范

1 范围

本文件规定了基于采用弱相干态光源的诱骗态 BB84 量子密钥分配产品的协议实现要求和产品基本要求的检测内容和方法。

本文件适用于指导符合 GM/T 0108—2021 研制的诱骗态 BB84 量子密钥分配产品的检测，也可用于指导研制。基于量子密钥分配产品的系统安全及其经典信道网络安全不属于本文件规定的范围。

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 2423.1 电工电子产品环境试验 第 2 部分：试验方法 试验 A：低温

GB/T 2423.2 电工电子产品环境试验 第 2 部分：试验方法 试验 B：高温

GB/T 5080.7 设备可靠性试验 恒定失效率假设下的失效率与平均无故障时间的验证试验方案

GB/T 15843.2 信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的机制

GB/T 15843.4 信息技术 安全技术 实体鉴别 第 4 部分：采用密码校验函数的机制

GB/T 15852.1 信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制

GB/T 15852.2 信息技术 安全技术 消息鉴别码 第 2 部分：采用专用杂凑函数的机制

GB/T 15852.3 信息技术 安全技术 消息鉴别码 第 3 部分：采用泛杂凑函数的机制

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38625 信息安全技术 密码模块安全检测要求

GM/T 0062 密码产品随机数检测要求

GM/T 0108—2021 诱骗态 BB84 量子密钥分配产品技术规范

GM/Z 4001 密码术语

3 术语和定义

GB/T 37092、GM/T 0050 和 GM/Z 4001 界定的术语和定义适用于本文件。

3.1

安全增强 privacy amplification

发送端与接收端对纠错后密钥进行数学处理，从中提取共享密钥的过程。

3.2

BB84 协议 BB84 protocol

由 Charles Henry Bennett 和 Gilles Brassard 在 1984 年提出的量子密钥分配协议。

3.3

对基 basis sifting

也称作筛选，是指发送端与接收端进行基矢比对，双方只保留接收端测量过程与发送端发送过程时