ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0108—2021

诱骗态 BB84 量子密钥分配产品技术规范

Decoy-state BB84 quantum key distribution product technology 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、中国科学技术大学、中国人民解放军信息工程大学、科大国盾量子技术股份有限公司、中国电子科技集团第三十研究所、清华大学、北京大学、重庆大学、上海交通大学、北京邮电大学、南京邮电大学、哈尔滨工业大学、密码科学技术国家重点实验室、数据通信科学技术研究所、江苏亨通问天量子信息研究院有限公司、北京天融信网络安全技术有限公司、格尔软件股份有限公司。

本文件主要起草人：韩正甫、刘云、刘婧婧、苗春华、银振强、鲍皖苏、李宏伟、赵勇、徐兵杰、宋晨、凌杰、张启发、刘杰杰、王剑锋、龙桂鲁、郭弘、向宏、曾贵华、喻松、张一辰、王琴、李琼、韩琦、何远杭、黄伟、王宇、胡滨、苏琦、于宗文、李申、赵良圆、薛梦驰、李金国、赵梅生、唐世彪、彭翔、蔡斌、张春梅、黄鹏、郑强、费新伟。

引　言

量子密钥分配技术经历了多年的发展历程，已经得到广泛应用。其中，BB84 协议是由 Charles Henry Bennett 和 Gilles Brassard 在 1984 年提出的量子密钥分配协议，同时也是迄今为止最为成熟和应用最广的量子密钥分配协议，其理论安全性已得到严格的证明。为推动量子行业在我国信息安全领域的发展，本文件将涵盖采用弱相干态光源的诱骗态 BB84 协议及该类产品的要求规范。

诱骗态 BB84 量子密钥分配产品技术规范

1 范围

本文件基于采用弱相干态光源的诱骗态 BB84 协议，对协议各阶段的技术实现进行了规范，并对采用该协议的产品的设计提出了基本要求。

本文件适用于诱骗态 BB84 协议的量子密钥分配产品的研制和检测。

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 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 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

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0062 密码产品随机数检测要求

GM/Z 4001 密码术语

3 术语和定义

GB/T 37092、GM/T 0050 和 GM/Z 4001 界定的以及下列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

参数估计 parameter estimation

估算出量子比特误码率和相位误码率等参数的过程。

3.4

对基 basis sifting

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所使用了相同基