



# 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

行业标准信息服务平台

2021-10-18 发布

2022-05-01 实施

国家密码管理局 发布

## 目 次

|                       |    |
|-----------------------|----|
| 前言 .....              | I  |
| 1 范围 .....            | 1  |
| 2 规范性引用文件 .....       | 1  |
| 3 术语和定义 .....         | 1  |
| 4 符号和缩略语 .....        | 3  |
| 4.1 符号 .....          | 3  |
| 4.2 缩略语 .....         | 3  |
| 5 检测环境 .....          | 3  |
| 5.1 测试参考点 .....       | 3  |
| 5.2 检测环境 .....        | 4  |
| 6 检测内容.....           | 12 |
| 6.1 协议实现要求检测 .....    | 12 |
| 6.2 量子密钥分配产品检测 .....  | 16 |
| 7 检测方法.....           | 18 |
| 7.1 协议实现要求检测 .....    | 18 |
| 7.2 防攻击检测 .....       | 27 |
| 7.3 量子密钥分配产品检测 .....  | 30 |
| 8 合格判定.....           | 33 |
| 附录 A (资料性) 检测仪器 ..... | 34 |
| 参考文献 .....            | 35 |

行业标准信息平台

## 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。

行业标准信息服务平台