ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 45240-2025

Device-independent quantum random number generators

器件无关量子随机数发生器通用要求

Issued on: January 24, 2025 **Implemented on: August 1, 2025**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part

1.Structure and drafting rules for standardization documents" Drafting. Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents. This document was proposed and coordinated by the National Technical Committee on Quantum Computing and Measurement Standardization (SAC/TC578). This document was drafted by: Jinan Institute of Quantum Technology, Anhui Guoke Quantum Network Co., Ltd., University of Science and Technology of China, Tsinghua University China Information Security Evaluation Center, China Great Wall Technology Group Co., Ltd., Anhui Information Security Evaluation Center, China... Tian Quantum Technology Co., Ltd., Shanxi University, Shanghai Jiao Tong University, Shandong Guoke Quantum Communication Network Co., Ltd., Shanghai Institute of Science and Technology of China Institute of Microsystem and Information Technology, Institute of Software, Chinese Academy of Sciences, China Institute of Metrology, Shenzhen Guoxin Quantum Technology Co., Ltd. Co., Ltd., Beijing Zhongke Guoguang Quantum Technology Co., Ltd., and Shanghai Guodun Quantum Information Technology Co., Ltd. The main drafters of this document are. Li Minghan, Jiang Yangfan, Wang Minglei, Zhang Qiang, Zhang Jun, Nie Youqi, Zhang Xingjian, Li Dongdong, Shi Hongsong, Liu Hongwei, Yu Chunlin, Wu Jiajie, Liu Jingjing, Shen Heng, Yu Yu, Qi Wei, Miao Yajun, Zhang Weijun, Cao Weiqiong, Deng Yuqiang, Wang Yiqu, Zhao Yibo, Xie Shuxin. General requirements for device-independent quantum random number generators

1 Scope

China's national standard for device-independent quantum random number generators. Random numbers underpin every cryptographic system, and the difficulty has always been that you cannot test a number sequence for randomness - a well-designed pseudorandom generator, or a compromised one, passes every statistical test. Quantum generators derive their output from measurements whose outcome is random by physical law rather than by ignorance, which is a stronger footing; but in practice you are still trusting that the device works as described, which is what an attacker attacks. Device-independent generation removes that trust: by testing a Bell inequality violation in the device's own outputs, it certifies that the numbers are genuinely random without assuming anything about the internal hardware. The standard defines the terminology, describes the structure of such generators, and specifies their performance requirements, for use in their development and testing.

This document defines the terms and definitions of device-independent quantum random number generators and describes the structure of device-independent quantum random number generators. The structure is composed of a device and the performance requirements of the device-independent quantum random number generator are specified.

This document is applicable to the development and testing of device-independent quantum random number generators.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document. For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to This document. GM/T 0005-2021 Randomness Testing Specification

3 Terms and definitions

The following terms and definitions apply to this document.

3.1 Bell inequality Bell-type inequality A class of inequalities for testing local hidden variable theory between nodes.

3.2 Beltest A test to determine whether Bell's inequality (3.1) is satisfied.

3.3 For different events that do not communicate with each other, the distribution of their results needs to satisfy certain conditions.

3.4 entanglement source There is a particle source of quantum entanglement between the generated particles. Note

1.Quantum entanglement refers to a non-classical correlation property between the states of multiple physical systems. Note

2.There are different types of entangled sources, such as photon-based, atom-based, etc.

3.5 quantum state The state of a quantum system. [Source: GB/T 42565-2023, 3.1]