Computer Science and Application 计算机科学与应用, 2026, 16(2), 395-404
Published Online February 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.162068

Hans汉斯

面向典型密码学场景的量子随机数预测应用研究

韩　宇*，费洋扬

河南省网络密码技术重点实验室，河南　郑州

收稿日期：2026年1月6日；录用日期：2026年2月6日；发布日期：2026年2月14日

摘　要

随机数在信息科学、量子通信、区块链等多个领域发挥关键作用，密码学场景对其安全性与不可预测性提出极高要求。伪随机数存在被破译的潜在风险，而基于量子力学原理的量子随机数作为真随机数，具备高强度安全性，是当前极具发展前景的随机数源。本文围绕量子随机数的预测分析及其密码学应用展开研究，概述离散型与连续型量子随机数发生器的研究现状，指出主流方案偏重成码率提升却忽视原始数据质量的问题；介绍NIST SP 800-22等主流统计性检测标准，分析其局限性；重点探讨量子随机数预测在密码学典型场景的应用，在区块链共识机制中优化节点选择、主节点更替等环节，在全域哈希、加盐哈希等哈希加密函数中降低碰撞风险与信息泄露隐患，同时明确各类应用中的适配难点；设计并实现基于JAVA语言的移动端QRNG后处理程序并在手机上验证其可行性。本研究通过分析量子随机数发生器生成机制并拓展其密码学应用场景，支撑网络空间安全、物联网终端认证等领域提供高安全等级的量子随机数基础设施建设。

关键词

量子随机数，密码学，随机数预测，随机数应用

Research on the Application of Quantum Random Number Prediction for Typical Cryptographic Scenarios

Yu Han*, Yangyang Fei

Henan Key Laboratory of Network Cryptography Technology, Zhengzhou Henan

Received: January 6, 2026; accepted: February 6, 2026; published: February 14, 2026

*通讯作者。

文章引用: 韩宇, 费洋扬. 面向典型密码学场景的量子随机数预测应用研究[J]. 计算机科学与应用, 2026, 16(2): 395-404. DOI: 10.12677/csa.2026.162068

Abstract

Random numbers serve a pivotal role in diverse fields such as information science, quantum communication, and blockchain, with cryptographic scenarios demanding exceptionally high standards for their security and unpredictability. Pseudorandom numbers are inherently vulnerable to cryptanalytic attacks, whereas quantum random numbers (QRNGs)—as true random numbers grounded in the principles of quantum mechanics—exhibit robust security and emerge as a highly promising random number source in contemporary contexts. This study focuses on the predictive analysis of quantum random numbers and their cryptographic applications. It provides an overview of the state-of-the-art in discrete-variable and continuous-variable Quantum Random Number Generators (QRNGs), highlighting that mainstream schemes prioritize bit rate enhancement while overlooking the quality of raw data. The paper presents mainstream statistical testing criteria, exemplified by NIST SP 800-22, and elaborates on their inherent limitations. Special emphasis is placed on investigating the applications of quantum random number prediction in typical cryptographic scenarios: within blockchain consensus mechanisms, it optimizes key processes such as node selection and master node replacement; in hash encryption functions (including universal hashing and salted hashing), it mitigates collision risks and potential information leakage, while addressing the inherent adaptation challenges across various application contexts. Additionally, a JAVA-based mobile QRNG post-processing program is designed and implemented, whose feasibility has been validated on mobile platforms. By analyzing the generation mechanisms of QRNGs and expanding their cryptographic application scenarios, this research facilitates the development of high-security quantum random number infrastructure to support fields such as cyberspace security and Internet of Things (IoT) terminal authentication.

Keywords

Quantum Random Numbers, Cryptography, Random Number Prediction, Random Number Applications

1. 引言

1.1. 研究背景

随着信息科学技术的不断发展，随机数在现代社会的诸多应用领域发挥着重要作用，如生物化学系统的数值仿真、科学数字模拟、基础理工科测试乃至博彩游戏等[1] [2]。量子通信和区块链等新兴技术也需要随机数的深度参与，如量子通信中对基等多个环节都需要进行随机选取，区块链系统的各类共识机制也往往需要随机数的深度参与以随机选取重要成员或重要区块。

但是不同应用场景对随机数的性质需求不尽相同，一些场景要求随机数满足一定的统计特性即可，例如各种模拟仿真实验等；但另外一些场景则需要进一步考虑随机数的安全性和脆弱性，例如一旦随机数作为算法的初始密钥种子被攻击者有效预测或掌握，则会带来十分严重的安全问题或系统风险。

在现实生活中，伪随机数承受着来自多个层面的安全性威胁，甚至在其最理想状态下也会因为其所规约的密码算法的破译而被完全攻破，在目前抗量子密码算法迁移与部署的大背景下，那些存在潜在安全隐患的经典密码算法生成的伪随机数在理论上都存在被牵连破译的可能性。

实际上随机数除了可以用计算机算法生成的伪随机数外，还包括利用各类物理特性生成的真随机数。理想中的真随机数是一组无偏置的随机数序列，应具有较好的统计学性质和不可预测性质。其中统计性良好是指随机数在统计分布上十分均匀，能够达到有关统计学测试的各类指标；不可预测性是指即使能够得到一部分随机数，攻击者也无法以不可忽略的概率(高于理论猜测最高概率)对后续的随机数进行有效预测。

目前最为广泛接受的真随机数即包括基于量子力学原理产生的量子随机数(Quantum Random Number Generator, QRNG) [3]。区别于基于密码算法产生的伪随机数面临前向攻击/后向攻击/状态泄露等安全性风险，量子随机数是由各种量子物理特殊现象不断产生的真随机数，具有很高的随机性安全强度，也是目前发展前景最为广阔的一类真随机数。

1.2. 研究意义

量子随机数发生器是量子通信领域技术最为成熟、商业化程度最高的量子通信关键设备，目前其研发朝着无条件安全、芯片化方向发展，因其基于量子力学等物理真随机数广泛应用于所有量子通信系统，并可逐步扩展至需求高安随机性的传统信息安全系统，同时其芯片化技术已获得全面突破并可直接应用于量子安全手机、车联网系统等高价值移动端商业场景，未来市场规模潜力巨大。作为知名的欧洲量子信息设备厂商，瑞士 IDQ 公司已与欧洲多家银行开展量子随机数合作与应用，其量子随机数设备应用于德国法兰克福部署的量子安全传输城域网络，其量子随机数芯片已应用于韩国 SK 电信开发的量子安全手机和安全数据传输机制，并开启与传统汽车厂商的车联网安全赋能探索[4]。

在安全应用方面，量子随机数源或可取代现有的伪随机数源或者与现有的伪随机数源通过某类数学算法混合而生成目前安全等级最高的随机数源，从而为长距离安全保密通信、网络空间系统安全维护、物联网终端设备安全认证与管理提供重要的随机数源基础设施和安全保障。

开展量子随机数预测分析研究主要切合量子随机数未来两方面的安全应用前景：一是在网络空间应用方面，全面提升量子随机数及其应用场景的安全性。具体而言，通过机器学习方法建立量子随机数预测模型，定量化深入研究量子随机数生成过程中种种因素对于随机数原始数据质量的影响，并有可能将现有模型无法精确评估的经典噪声、采样带宽等因素对最终随机性的影响纳入模型评估，进而对量子随机数的生成过程进行环节完善与参数修正，查找漏洞、补足短板，对物理安全模型以及随机数生成速率公式进行检验和完善，指导优化实验设置和关键参数设计，从而提升量子随机数自身的安全性及其应用场景的安全性。二是在网络空间防御方面，开展基于量子随机数分析的典型密码场景安全测试。具体而言，通过机器学习方法建立量子随机数分析模型，查找现有不同技术方案的量子随机数发生器有可能存在的安全漏洞与隐患，分析目前量子随机数在密码学和通信中的应用场景，找出其中典型的密码学与通信协议，例如哈希函数、区块链、量子通信等，将量子随机数的机器学习用于上述协议中并分析对安全性造成的影响。

2. 基于可信设备的量子随机数发生器概况

2.1. 基于可信设备的量子随机数发生器研究现状

可信任的量子随机数发生器主要包括两类，分别是离散型变量和连续型变量的量子随机数发生器。其中，离散型变量的量子随机数发生器充分利用诸如光子到达时间、光子数分辨、光子到达空间分辨等各种独立的物理信息，其特点是结构简单、后处理方便，适合小型化；缺点是受到带宽和探测器效率的限制，产生随机数的速率较低并且很难提升，因此是早年理论方案清晰、实现难度较低的生成方案，但因其较弱的可扩展性和较低的随机数生成码率而被逐渐放弃。

而连续变量随机源是指其物理源输出是连续的，目前的主流方案主要包括放大自发辐射噪声、激光相位噪声及真空散粒噪声等等，在主要结构上主要包含量子熵源、量子探测、经典采样、经典后处理等四个部分。由于相位噪声的模型研究较为彻底，主要利用高速的光电探测器测量系统的量子随机性，且可以在后处理过程中有效地对随机性提取理论进行分析而得到随机性更好的序列。同时，连续型变量量子熵源发生效率和测量效率均高于离散型变量量子熵源，因此极大地提高了随机数的生成速率，该特点也使得连续型变量量子随机数发生器成为目前量子随机数发生器的研究重点。

真空散粒噪声方案方面，C. Gabriel 等人实现了基于真空涨落的 QRNG 方案[5]，其利用零差探测技术提取真空散粒噪声中的量子随机信息，从而输出量子随机数。虽然该方案的量子特征明显并且理论上真空噪声具有无限带宽，但是实际中的经典噪声不易消除，同时制备高带宽的零差探测器困难，极大地限制了随机数的生成速率，最高也只能达到 Gbps 量级，从而限制了后续研究的进一步深入。

激光相位噪声方案方面，郭弘小组提出并实现基于激光相位噪声的 QRNG 方案[6]，利用拍频测量技术把自发辐射噪声转换为强度噪声，其基本原理是利用激光中的自发辐射噪声引起激光场的相位涨落，实现对激光的相位噪声的有效探测，输出量子真随机数。Nie 等人实现了基于相位噪声量子随机数发生器方案，得到了 68 Gbps [7]的离线随机数生成速率以及 3.2 Gbps [8]的在线随机数生成速率。目前，在基于激光相位噪声的 QRNG 方案中，Ren 小组提出的方案在最高的实时随机数生成速率可达 117 Gbps [9]。

放大自发辐射噪声(amplified spontaneous emission, ASE)方案方面，Williams 等人提出并首次实现基于 ASE 噪声的 QRNG 方案[10]，其利用掺铒光纤放大器作为量子光源，由光纤偏振分束器把光噪声分为两路相同的光噪声信号，经过光电探测器和误码仪采样，可以离线产生速率为 12.5 Gbps 的随机数。其中，超辐射发光二极管(super-luminescent emitting diode, SLED)是一种基于 ASE 噪声的随机源，具有稳定性好、大带宽、输出的 ASE 噪声易于测量等优点，逐渐成为放大自发辐射噪声的研究主流方案。X. Li 等人提出使用 SLED 的两组中心波长不同的滤波谱 ASE 噪声产生量子随机数[11]，每组 ASE 噪声都可以产生 10 Gbps 的随机数，最终实现了两路并行的 QRNG 方案。

总体来说，量子随机数发生器应用前景十分广泛，各种类型的理论方案不断更新迭代，但目前的主流方案均以获得越来越高的最终随机数成码率为极其重要的评价指标。因为成码率的比较十分直观显然，也是衡量随机数实际功效的重要因素；但是缺乏对量子随机数在后处理过程前的原始数据质量的横向比较。由于量子随机数的后处理过程一般都通过现场可编程门阵列(FPGA)实现，如果其后处理种子也是相对固定的，量子随机数的最终数据质量就直接与后处理过程前的原始数据质量直接相关，而目前相关的研究是十分匮乏的，很多量子随机数发生器方案在设计过程中也少有提到或比较原始数据的质量问题，这是一个突出部分最终数据亮点(高成码率)而忽视关键环节(原始数据的脆弱性)的危险现象，量子随机数发生器研究领域的长远健康发展应当实现量与质的兼顾。

2.2. 量子随机数的统计性检测方法

2010 年，美国国家标准局对外公布了随机数测试标准的新版本。NIST SP 800-22 是美国国家标准局发布的关于随机数性能标准的指南，研究人员认为这是目前随机数领域较好的评价标准[12]。国家标准局测试集面向基于硬件或软件密码的物理随机或伪随机数生成器所产生的二进制序列。

该版本共定义了 15 个测试项，主要包括：单比特频数测试，检测序列中 0、1 个数是否相等；块内频数测试，检测各个块内序列中 0、1 个数是否相等；游程总数测试，0、1 游程检测；块内最大游程测试，检测块内 1 最大游程；矩阵秩测试，检测确定长度的子序列以及其线性相关性；离散傅立叶测试，序列周期方面的主要性质，与真随机进行比较；非重叠块的匹配测试，检测子序列与非重叠模板相似程度；重叠块的匹配测试，检测定长序列 1 游程的个数；通用统计检测，检测序列是否可以在保存完整信

息的情况下被压缩；线性复杂度测试，检测序列的复杂度；重叠子序列测试，检测 m 长比特串出现次数是否与真随机序列中的情况近似相同；近似熵测试，检测 m 与 m − 1 长度的比特串在等待检测序列中的出现频率，并与正态分布序列中的情况进行比对；累加和测试，检测序列部分和的大小；随机偏移测试，检测某个特定状态出现次数为 K 的 cycle 个数；随机偏移向量测试，检测游程内特定状态出现的总次数与真随机序列的偏离程度。

2012 年，我国国家密码管理局发布了 GM/T 0005-2012 统计性检测标准。国产商用密码应用中随机数发生器产生的二进制序列需要通过该检测。该规范包含了 15 种随机数检测算法。其中，多数检测项方法与 NIST SP 800-22 标准相同，不同的测试项如下：扑克检测，检测子序列是否与太多的非重叠模板相匹配；二元推导检测，通过依次将初始序列中相邻的两比特异或得到新序列，检测经过 k 次后，0、1 个数是否相近；自相关检测，检测序列与其逻辑左移 d 位后的新序列的相关程度。

目前主流的量子随机数设计方案均以是否通过国家标准局或 GM 统计性测试来证明其安全性的实现。但实际上，统计性良好并不意味着不可以被有效预测。同时，统计性预测的方法只能给出该类随机数设计方案通过或不通过的定性结论，无法针对不通过的具体原因展开定性分析以有效评估影响最终随机性生成的重要因素进而不断完善整个量子随机数制备设计方案。

3. 典型密码学场景中的量子随机数预测分析应用与实现

量子随机数因其真随机性而可以广泛应用于密码学和数据科学等各个领域，尤其在区块链安全性提升和哈希加密函数方面有着重要应用前景。在区块链领域，量子随机数可优化共识机制中的节点选择、主节点更替等环节，替换传统确定性随机数生成方案，规避核心参数泄露风险，同时需适配不同节点类型、使用环境及主流量子随机数产生方案，解决网络扩展、芯片化集成等适配难点。在哈希加密函数应用中，量子随机数可降低全域哈希与加盐哈希的碰撞风险及信息泄露隐患，但量子随机数发生器的设备漏洞可能导致随机性不足，引发安全问题。

3.1. 量子随机数在区块链系统中的应用及预测性风险分析

自 2008 年中本聪首次提出区块链概念以来，区块链技术及其落地应用实现了高速发展，以比特币、以太坊、HyperledgerFabric、Cardano 等为代表的区块链项目，已在支付清算、供应链金融、数字身份认证等多个领域形成规模化应用。高质量随机数能够显著提升区块链共识机制的随机性、可扩展性、鲁棒性与共识效率，为区块链系统的安全运行提供更高等级的保障。量子随机数发生器(QRNG)在区块链共识机制中具备广泛的应用价值，随机共识机制的核心原理，是将传统共识机制中的随机数生成算法替换为安全等级更高的实现方式，以此抵御攻击者针对随机数生成阶段发起的恶意攻击。此外，部分新型共识机制本身即属于随机共识机制范畴，典型如专注于高吞吐量的 Algorand 公链采用的“纯权益证明”(本质为随机共识机制)、基于随机森林算法优化的联盟链共识方案等，与随机工作量证明(RPOW)、随机权益证明共识(RPOS)共同构成主流随机共识体系；而比特币采用的工作量证明(POW)、以太坊合并后采用的权益证明(POS)等传统共识机制，在核心环节同样依赖随机数生成——比特币挖矿过程中区块哈希值的生成需引入随机扰动保证出块公平性，以太坊 POS 共识中验证者节点的随机选举也离不开可靠随机数支撑。总体而言，随机数的生成质量与共识机制的安全等级呈正相关，生成的随机数质量越高，共识机制的安全性与公平性就越有保障。

高质量随机数为随机共识机制提供技术支撑的具体方案主要分为两类：其一为本地搭载量子随机数可信设备，包含内置式与外置式两种部署形态，该方案更适用于联盟链、私有链等对数据安全性要求极高且节点可控的场景，例如金融机构基于 HyperledgerFabric 搭建的供应链金融区块链平台，可在核心验

证节点本地内置量子随机数发生器，保障交易共识的安全可控；其二为搭建基于可信网络传输的量子随机数源公共软件接口服务，更适配节点分布广泛、硬件改造难度大的公链场景，如 Cardano 公链可通过接入第三方量子随机数公共接口，为全网节点提供统一的高安全随机数服务。两类方案的核心目标一致，即替代传统的确定性随机数生成方案，从根源上规避因核心参数或初始密钥泄露引发的随机数生成安全漏洞，为区块链共识机制提供高安全性、高不可预测性的量子随机数。

将量子随机数技术应用于区块链共识机制的实际落地，除上述算法设计外，仍需突破诸多技术难点。在不同的区块链共识场景中，不同类型节点与不同业务环节均存在差异化的随机数生成需求，因此量子随机数生成技术的落地适配，需紧密结合共识关键环节中对应节点的实际需求开展优化设计。例如，比特币全节点多为个人用户搭载的普通服务器，难以额外搭载硬件模块，需适配轻量化量子随机数获取方案；而联盟链核心节点多为机构可控的高性能物理机，可直接外置量子随机数设备提升安全性。同时，还需根据实际使用环境(随机数在使用与处理前是否处于安全存储空间、节点为离线或在线运行状态、业务流程中是否有用户参与等)，针对性调整技术方案。当前，量子随机数在区块链共识机制中的潜在应用场景主要包括：将量子随机数源应用于共识协议参与者随机选择、主节点随机更替、数据一致性校验等核心环节，如 Dash (达世币)公链的主节点轮换选举、以太坊 2.0 分片网络的验证者分配等步骤；基于量子随机数源技术满足大容量区块链网络扩展及节点身份识别的实际需求，适配 Polygon、Arbitrum 等 Layer2 扩容网络的海量节点随机调度需求；实现基于真空涨落、相位噪声、自发放大辐射噪声、光强涨落等主流可信设备的量子随机数产生方案，与区块链各类应用场景的技术适配；完善量子随机数最小熵估计的理论框架与参数设计方案；优化随机数后处理过程中的矩阵规模设计与密钥文件选取策略；推进量子随机数发生器的小型化与芯片化设计开发；实现小型化量子随机数发生设备与实际运行的区块链系统服务器等实体设备的集成搭载；为区块链节点提供外接量子随机数源的硬件适配与技术支持；搭建适配现代网络传输条件的量子随机数源公共软件接口服务体系。

现有区块链系统在随机数安全层面仍存在诸多潜在隐患，其中核心问题之一是部分系统采用确定性随机数生成方案，这类方案高度依赖区块链运行过程中的各类系统参数，存在显著的可预测性风险。除 EOS 生态中的 EOS.WIN 游戏项目外，早期部分小型公链(如某匿名支付公链)也曾因采用基于区块高度、交易哈希的确定性随机数生成方案，被攻击者破解参数后操控共识结果，导致双花攻击事件。以 EOS.WIN 项目为例，该项目中用户通过输入数字猜测大小，与系统生成的随机数比对后，猜中即可获得相应收益；显然，若攻击者能够操控系统生成的随机数，便可通过恶意套利获取不当利益。该项目的随机数由一套确定性算法生成，其核心计算参数涵盖交易哈希 ID、成交区块高度、成交区块前缀、全局开奖序号等区块链系统运行参数，攻击者可通过精心设计的攻击手段窃取上述参数，进而实现对随机数生成结果的操控，最终达成套利目的。即便是比特币、以太坊等主流区块链，其随机数生成环节也存在潜在风险——比特币的区块哈希生成虽依赖算力竞争引入随机性，但仍存在攻击者通过大规模算力控制影响随机结果的可能；以太坊 POS 共识的随机数生成依赖节点提交的“随机 beacon”，若提交节点存在恶意串通，可能降低随机数的均匀性。若区块链系统的随机数生成质量不佳，如某节点生成的随机数存在明显的可预测性特征，不仅会让系统丧失安全运行的基础，更无法保障共识过程的公平性。此外，将量子随机数与抗量子公钥算法进行融合应用，可作为非交互式零知识证明的高安全随机数源，同时为区块链身份认证环节提供高安全性的技术支撑，该融合方案可广泛推广至现有各类区块链系统，如用于比特币的地址身份认证优化、HyperledgerFabric 的节点准入验证等，显著提升系统的整体安全防护能力。

在具体应用落地层面，基于可验证随机函数(VRF)的量子增强共识算法是量子随机数发生器(QRNG)与区块链共识机制融合的典型实现方案。该方案将 QRNG 生成的真随机数作为 VRF 的核心种子，既完整保留了 VRF 本身的可验证性与确定性核心优势，又依托量子随机数的高熵特性，大幅提升区块链共识

过程的抗攻击能力，其具体实施流程设计如下：

1) 初始化阶段：节点备案与 QRNG 部署。全网验证节点完成身份注册后，生成基于格基密码 NTRU 算法的抗量子公钥对并上链备案；为各节点部署轻量化 QRNG 模块，其中公链节点适配外置 USB 式 QRNG 设备，核心节点搭载内置芯片式 QRNG，同时搭建“QRNG-节点”可信通信通道，保障量子随机数传输的防篡改、防窃取性，全网同步约定 VRF 函数模板、节点私钥及 QRNG 生成的输入随机种子相关规范。

2) 随机种子生成与同步阶段：QRNG 分布式赋能。各验证节点通过本地 QRNG 生成 128 位真随机数，经自身抗量子公钥加密后，将加密结果与节点身份标识一同全网广播；全网节点收集所有加密信息后，通过多方安全计算(MPC)协议完成异或聚合，生成全网统一的全局随机种子，该方式可确保单节点随机数泄露不影响全局安全性，且聚合全过程由智能合约自动执行并上链留痕。

3) VRF 计算与领导者选举阶段：可验证随机筛选。各验证节点将全局随机种子作为 VRF 输入参数，代入本地 VRF 函数完成计算，全网依据节点输出的“随机竞争力值”进行升序排序，选取前若干节点作为本轮共识出块领导者；各节点同步将计算结果与验证信息全网广播，其他节点可通过对应节点公钥快速验证结果有效性，及时剔除伪造随机结果的恶意节点。

4) 共识确认与种子更新阶段：全流程安全闭环。当选的领导者节点完成交易打包与区块生成后，将区块哈希与本轮全局随机种子绑定上链，实现共识结果与随机种子的关联校验；进入下一轮共识周期前，各节点通过本地 QRNG 重新生成随机数种子，重复种子聚合、VRF 计算与领导者选举流程，通过种子的实时更新规避复用带来的安全风险。

该方案通过 QRNG 与 VRF 的融合实现了安全与效率的适配平衡，其中安全性提升与硬件成本的权衡关系尤为显著：相较于传统依托伪随机数的 VRF 方案，QRNG 产出的真随机数种子熵值超 128 位，能有效抵御生日攻击、暴力破解等伪随机数种子预测类攻击，结合抗量子公钥技术，还可从源头规避量子计算机对 RSA、ECDSA 等传统密钥的破解隐患；但在成本端，公链海量节点部署 QRNG 设备将产生额外的硬件采购与运维开支，核心节点开展芯片式 QRNG 的内置集成改造，还需配套投入研发资源，因此该方案更适配金融公链、联盟链这类对安全等级要求严苛的区块链场景。

3.2. 量子随机数在哈希加密函数中的应用及预测性风险分析

哈希加密函数是当代密码学领域的常用工具。常见的哈希函数包括 MD5、SHA 系列(SHA-1、SHA-256、SHA-3)、CRC32 等，其中 SHA-256 在区块链、数字签名等安全场景中应用最为广泛。这类哈希函数能将任意长度的原始数据高效且不可逆地映射为固定长度的短数据，例如 MD5 输出 128 位(32 个十六进制字符)哈希值，SHA-256 输出 256 位(64 个十六进制字符)哈希值，且对原始数据的微小扰动(比如修改一个字符)，都会使哈希函数的映射结果产生雪崩式的显著变化。通过存储并对比两组不同来源数据经同一哈希函数运算后的结果，可轻松判断两组数据是否一致；但想要通过哈希值反推原始数据，仅能通过暴力枚举原始数据并计算哈希值逐一比对的方式验证，该过程所需计算量为数据规模的指数级别，在当前算力条件下无法实现(例如想要反推一个 SHA-256 哈希值对应的原始字符串，几乎不具备可行性)。由于哈希函数是将大空间的数据编码至固定大小的小空间中，因此存在小概率的哈希冲突，即两个不同的原始数据生成相同的哈希值。一款设计优良的哈希函数，需将哈希冲突的概率控制在极低水平，也就是让不同数据尽可能均匀地映射至各个哈希值上——例如 SHA-256 的哈希冲突概率远低于 MD5，这也是 MD5 逐渐被淘汰出安全场景的重要原因。但即便如此，也无法保证该哈希函数对任意数据子集，都能实现向各个哈希值的均匀映射，而全域哈希恰好解决了这一问题。全域哈希依托一族彼此独立的哈希函数，每次对数据进行哈希映射时，算法会从该哈希函数族中随机选取一个函数完成运算，并将运算结果作为

该数据的哈希值。只要能保证，对于任意两组不同数据，哈希函数族中会使其产生哈希冲突的函数占比极低，即可认为全域哈希算法生成的哈希值分布具备均匀性。

全域哈希通过在哈希函数的选取环节引入随机性，确保原始数据的任意子集都能均匀映射至各个哈希值，从而最大限度降低哈希冲突的概率。但全域哈希算法并未保证哈希函数族中的单个哈希函数，其输出的哈希值本身具备均匀分布特性，甚至部分单个哈希函数可能存在性能缺陷——例如某全域哈希函数族中包含类似 CRC32 的简单哈希函数，该函数在处理连续数字类数据子集时，哈希分布会出现明显偏差。在实际算法应用中，每次对数据进行哈希加密时，哈希函数的随机选取均依赖随机数生成器，而随机数生成器的引入则带来了新的安全威胁。攻击者可通过量子随机数预测攻击，预判数据子集后续哈希映射所使用的哈希函数，进而从哈希函数族中筛选出性能缺陷的函数，以此预测哈希运算结果；情况严重时，甚至可通过这类函数反推出原始数据的部分信息，最终造成信息泄露。

在哈希函数体系中，全域哈希函数是一种随机化的哈希方法，核心设计目标为降低哈希碰撞概率。通过随机选取哈希函数的方式，全域哈希函数能保证任意两个不同输入产生哈希碰撞的概率极低，这一特性使其尤为适用于对安全性要求较高的场景，如密码学应用、数据完整性验证等。目前全域哈希函数在密码学领域的应用已十分广泛，例如在数字签名构建中，常将 SHA-256 或 SHA-3 与全域哈希函数结合，大幅提升签名的安全性，使攻击者无法预知或操控哈希值，从而降低 RSA、ECDSA 等签名算法被伪造的风险；在比特币等区块链的安全交易场景中，通过基于 SHA-256 构建的全域哈希函数处理交易信息，可有效保障每笔交易的唯一性与不可篡改性。随机数在全域哈希函数中的应用可概括为：每次生成哈希值时，通过高质量随机数生成器从哈希函数族中随机选取哈希函数，让每次哈希运算都具备唯一性，这种随机性能够有效抵御针对固定哈希函数(如早期的 MD5)的碰撞攻击。

加盐哈希函数是在传统哈希函数的输入端加入随机生成的盐值(一串随机数)，以此增强哈希输出结果的安全性。目前工程实践中，常用的加盐哈希实现方案多基于成熟哈希函数扩展，例如 bcrypt (基于 Blowfish 算法扩展，内置盐值生成)、Argon2 (密码学竞赛获胜算法，支持自定义盐值与算力消耗)、PBKDF2 (基于 SHA-256、HMAC 等哈希函数构建)。

盐值的核心作用除了带来熵增益，还能避免使用相同原始数据的用户，生成相同的哈希值，从而大幅降低攻击者通过彩虹表等方式进行暴力破解的概率。在实际应用中，密码存储领域：用户注册时，系统会随机生成真随机数盐值并与用户密码结合，经 bcrypt 或 Argon2 哈希处理后将结果存储于数据库；即便攻击者获取到该哈希值，也无法直接反推出原始密码。此外在 API 密钥管理中，PBKDF2 (基于 SHA-256)也被广泛用于用户密钥的存储，即便不同用户使用相同的原始密钥，也会因真随机数盐值的随机性生成不同的哈希值，进一步提升密钥存储的安全性。

工程实践中，量子真随机数盐值的比特长度选择会兼顾熵增益与系统运行成本，主流的 16 比特、32 比特量子真随机数盐值是防御效果与成本的最优平衡点：16 比特盐值带来 16 比特熵增益，在硬件资源、哈希计算耗时几乎无增加的前提下，让彩虹表攻击的成本提升 2^{16} 倍(65,536 倍)；32 比特盐值带来 32 比特熵增益，攻击成本提升 2^{32} 倍(约 42 亿倍)，仅需少量硬件资源消耗，即可实现对彩虹表攻击的绝对防御。而 64 比特及以上的真随机数盐值，虽能带来更高的熵增益，但会增加哈希计算与存储的额外开销，且 32 比特熵增益已足够让彩虹表攻击失去技术可行性，因此无需过度提升盐值长度。量子真随机数盐值的熵增益可通过其比特长度精准量化，且为无冗余的纯增量，该增益通过指数级推高彩虹表攻击的预计算存储量与计算量，从技术层面实现了对彩虹表攻击的有效防御；而真随机数的信息独立性，让其熵增益能完全转化为抗攻击能力。

在随机性预测攻击场景中，若量子随机数发生器存在设备漏洞，其输出的随机数实际随机性会低于理论估计值，将此类随机数应用于全域哈希函数(如基于 SHA-256 构建的全域哈希族)和加盐哈希函数(如

bcrypt、Argon2)时，会引发严重的安全隐患。对于一类特殊的全域哈希函数，其性能还会受基于随机种子的随机性提取器影响：当随机种子的实际随机性被高估时，提取器的输出随机性会大幅下降。强双源搅拌器作为一种特殊的随机性提取器，同样存在此类问题——当搅拌器的任意一个输入源的随机性被高估时，其输出的随机哈希值与均匀分布的偏差会显著增大，最终影响以 SHA-256、SHA-3 为核心的哈希函数的安全性。

3.3. 量子随机数后处理的移动端实现

量子随机数的小型化乃至芯片化制程工艺成为其近年来的重要发展趋势，如果能将量子随机数发生器的原始数据生成部分通过芯片化实现，理论上的后处理过程可以在手机端完成，这将加速量子随机数芯片在移动端的应用。本文设计了基于 JAVA 语言的量子随机数后处理程序实现，可用于支持量子随机数原始数据在移动端的后处理操作，避免了 FPGA 电路板的体积限制，展现出在移动端的潜在应用前景。

具体而言，开发了量子随机数的移动端后处理程序，支持安卓手机终端为载体，支持最常见的 Toeplitz 矩阵为实现后处理程序的最基础算法，支持随机生成或选取指定文件作为 Key 数据，如图 1 所示；提供中英文操作界面；支持最大 10M 的文件单次处理以及最多 100 个文件的批处理功能；支持数据看板、实时监控计算进度以及内存使用率图表、分析设备计算力等功能。这将加速并扩展量子随机数芯片在手机、平板等移动端的应用。

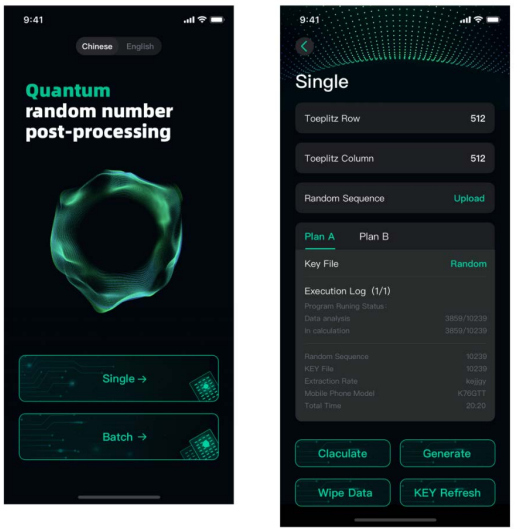

Figure 1. Schematic diagram of the post-processing system for quantum random numbers on mobile terminals
图 1. 移动端量子随机数后处理系统示意图

在华为 MATE60 手机上使用 1024 × 2048 的 Toeplitz 矩阵，对 4 M 左右的随机序列进行处理，时间大概在 40 秒；使用小规模后处理矩阵会使时间明显缩短。目前已经验证了手机端的量子随机数后处理的可行性，下一步将继续进行各种程序优化、资源占用计算并使用快速傅里叶变换开展测试。

4. 结语

本文围绕量子随机数的预测分析及其密码学应用展开系统研究，重点探讨量子随机数在区块链共识机制(优化节点选择等环节)与哈希加密函数(降低碰撞风险)中的典型应用及适配难点，同时设计实现基于 JAVA 语言的移动端后处理程序，为高安全随机数基础设施建设提供支撑。未来可进一步优化量子随机

数原始数据质量与成码率的平衡，深化多密码学场景的适配方案，推进发生器芯片化与小型化技术迭代，完善移动端程序的性能与兼容性，加强与抗量子算法的融合应用，助力量子随机数在车联网、物联网等更多高安全需求领域实现规模化商业化落地。

参考文献

[1] Zhang, J., Zhang, Y., Zheng, Z., Chen, Z., Xu, B. and Yu, S. (2021) Finite-Size Analysis of Continuous Variable Source-Independent Quantum Random Number Generation. *Quantum Information Processing*, **20**, Article No. 15. https://doi.org/10.1007/s11128-020-02936-7

[2] Michel, T., Haw, J.Y., Marangon, D.G., Thearle, O., Vallone, G., Villoresi, P., *et al.* (2019) Real-Time Source-Independent Quantum Random-Number Generator with Squeezed States. *Physical Review Applied*, **12**, Article ID: 034017. https://doi.org/10.1103/physrevapplied.12.034017

[3] Zhou, H., Yuan, X. and Ma, X. (2015) Randomness Generation Based on Spontaneous Emissions of Lasers. *Physical Review A*, **91**, Article ID: 062316. https://doi.org/10.1103/physreva.91.062316

[4] Imran, M., Sorianello, V., Fresi, F., Potì, L. and Romagnoli, M. (2020) Quantum Random Number Generator Based on Phase Diffusion in Lasers Using an On-Chip Tunable SOI Unbalanced Mach-Zehnder Interferometer (uMZI). *Optical Fiber Communication Conference* (*OFC*) 2020, San Diego, 8-12 March 2020, 1-3. https://doi.org/10.1364/ofc.2020.m1d.5

[5] Gabriel, C., Wittmann, C., Sych, D., Dong, R., Mauerer, W., Andersen, U.L., *et al.* (2010) A Generator for Unique Quantum Random Numbers Based on Vacuum States. *Nature Photonics*, **4**, 711-715. https://doi.org/10.1038/nphoton.2010.197

[6] Guo, H., Tang, W., Liu, Y. and Wei, W. (2010) Truly Random Number Generation Based on Measurement of Phase Noise of a Laser. *Physical Review E*, **81**, Article ID: 051137. https://doi.org/10.1103/physreve.81.051137

[7] Nie, Y., Huang, L., Liu, Y., Payne, F., Zhang, J. and Pan, J. (2015) The Generation of 68 Gbps Quantum Random Number by Measuring Laser Phase Fluctuations. *Review of Scientific Instruments*, **86**, Article ID: 063105. https://doi.org/10.1063/1.4922417

[8] Zhang, X., Nie, Y., Zhou, H., Liang, H., Ma, X., Zhang, J., *et al.* (2016) Note: Fully Integrated 3.2 Gbps Quantum Random Number Generator with Real-Time Extraction. *Review of Scientific Instruments*, **87**, Article ID: 076102. https://doi.org/10.1063/1.4958663

[9] Ren, M., Wu, E., Liang, Y., Jian, Y., Wu, G. and Zeng, H. (2011) Quantum Random-Number Generator Based on a Photon-Number-Resolving Detector. *Physical Review A*, **83**, Article ID: 023820. https://doi.org/10.1103/physreva.83.023820

[10] Williams, C.R.S., Salevan, J.C., Li, X., Roy, R. and Murphy, T.E. (2010) Fast Physical Random Number Generator Using Amplified Spontaneous Emission. *Optics Express*, **18**, 23584-23597. https://doi.org/10.1364/oe.18.023584

[11] Li, X., Cohen, A.B., Murphy, T.E. and Roy, R. (2011) Scalable Parallel Physical Random Number Generator Based on a Superluminescent Led. *Optics Letters*, **36**, 1020-1022. https://doi.org/10.1364/ol.36.001020

[12] Fei, X., Yin, Z., Cui, C., Huang, W., Xu, B., Wang, S., *et al.* (2018) Optimality of Quantum Randomness Certification with Independent Devices. *Journal of the Optical Society of America B*, **35**, 2186-2191. https://doi.org/10.1364/josab.35.002186