Chronos

ALEA16
1.6 Gbps, Research-Grade
True Random Number Generator

ALEA16 ALEA16 随机性测试数据

TR-03-1-010-1, Nov. 2026

Chronos Technology specializes in the development of ultra-high precision measurement equipment, offering nanosecond-level synchronization solutions tailored for the quantum, medical, and industrial sectors. For more product information, please visit our official website- *www.chronosci.com*

Chronos

Copyright Notice

Copyright © 2026 by Chronos Technology Inc. All rights reserved.
This document contains information that is proprietary and confidential to Chronos Technology Inc. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher.

1. 典型测试电路和测试结果

10.1 测试简介

本章主要介绍 ALEA16 系统的测试方案与核心结果。

由于 ALEA 采用了 RO 振荡器和 FPGA-TDC 技术，且每个通道电子噪声有所差异，因此本章的测试结果仅做参考典型值。实际每一台的性能官方会提供一份质量检验报告，用户具体所选购的设备具体性能可以参考质量检验报告。

除温度测试外，所有测试在实验室常温（~25 ℃）环境下进行。

10.2 RO 周期测试

由于 ALEA 采取了 RO 方式作为熵源，每个设备、每个通道的计数率会有不同。如下表是一个设备各个通道的典型测试结果。

表格 1 各通道熵比特率（典型结果）

通道号	计数率，Mbps
1.	112.3
2.	111.7
3.	100.5
4.	107.6
5.	107.2
6.	107.5
7.	120.1
8.	119.5
9.	120.5
10.	109.3
11.	111.4
12.	114.8
13.	111.9
14.	115.9
15.	125.3
Total	1695.5

实际采集数据量统计：

对于熵源数据模式，系统采集 2s 数据，采集 10 次，平均每次可以采集到 435000KB 随机数，即熵源随机数率约为 1.7 Gbps；

对于 SM3 数据模式，系统采集 2s 数据，采集 10 次，平均每次可以采集到 340000KB 随机数，即熵源随机数率约为 1.4 Gbps；

10.3 熵源输出测试

熵源模式，ALEA 输出没有经过任何后处理的随机数据流。

10.3.1 NIST SP 800-90B 测试

NIST SP 800-90B《Recommendation for the Entropy Sources Used for Random Bit Generation》是美国国家标准与技术研究院（NIST）于 2018 年发布的熵源评估标准，与 SP 800-90A（DRBG）和 SP 800-90C（RBG 构造）共同构成随机数生成器的完整规范体系。该标准将熵源划分为噪声源、健康检测和调理三个部分，并要求通过统计估计给出熵源的最小熵下界：若熵源通过 IID 检验，则采用 IID 轨（以 MCV 估计）；否则采用 non-IID 轨，用 MCV、Collision、Markov、Compression、t-Tuple、LRS、MultiMCW、Lag、MultiMMC、LZ78Y 共 10 个估计器分别估计并取最小值。标准同时规定了启动检测与连续检测（RCT、APT）等健康检测机制，以及基于调理定理的熵值折算方法，是当前 TRNG 设计与认证领域最具影响力的评估依据之一。

10.3.1.1 IID 测试

为判断熵源是否满足独立同分布（IID）假设，NIST SP 800-90B 规定了一组统计检验。首先，卡方独立性检验用于检测样本之间是否存在相关性；卡方拟合优度检验用于检测样本分布是否偏离均匀分布；最长重复子串（LRS）检验用于检测数据中是否出现异常长的重复模式；置换检验则通过 19 种统计量（游程、碰撞、周期性、协方差、压缩等），将原始序列与随机置换序列进行对比，以判断其是否含有非随机结构。所有检验均在 1,000,000 个样本上执行，各检验的 p 值须高于标准规定的显著性水平，或通过规定的置换轮数判据。若全部检验通

过，则说明熵源满足 IID 假设，可采用 IID 轨、以最常值（MCV）估计最小熵；否则必须转入 non-IID 轨，由 10 个估计器分别估计并取最小值。因此，IID 检验不仅是对熵源统计质量的直接验证，也是决定后续熵估计方法的关键前提。

在室温下，ALEA 设备输出的熵源随机数 IID 测试结果如下表所示。最小熵为 0.994646 bit。

表格 2 IID 测试结果（熵源）

参数	值	说明
样本数	1000000	
Raw Mean	0.499429	原始均值
Median	0.5	中位数
Binary	TRUE	二值数据
MCV mode	500571	最常见值出现次数
MCV p-hat	0.500571	最常见值概率
MCV p_u	0.50185891	99% 上界
MCV H_original	0.994646	IID 轨最小熵
Chi-square independence score	2117.141997	独立性卡方统计量
Chi-square independence dof	2046	自由度
Chi-square independence p-value	0.133522	>0.01 通过
Chi-square goodness score	6.486204	拟合优度统计量
Chi-square goodness dof	9	自由度
Chi-square goodness p-value	0.690442	>0.01 通过
Chi-square tests	Passed	卡方测试结论
LRS P_col	0.500001	最长重复子串 P_col
LRS Length	37	最长重复子串长度
LRS Pr(X>=1)	0.973692	LRS 概率
LRS test	Passed	LRS 结论
Permutation tests	Passed (19/19)	置换检验结论
Overall IID	Passed	总体结论

10.3.1.2 non_IID 测试

当熵源未能通过 IID 检验，或其统计特性不宜作独立同分布假设时，NIST SP 800-90B 要求采用 non-IID 轨进行熵估计。该轨不依赖 IID 假设，而是从多个角度对序列进行最坏情况分析：MCV 估计最常值概率，Collision 估计碰撞概率，Markov 估计一阶马尔可夫转移概率，Compression 估计序列的可压缩性，t-Tuple 与 LRS 分别从短元组和最长重复子串的角度刻画局部重复结构，MultiMCW、Lag、MultiMMC 和 LZ78Y 则通过多种预测器评估序列的可预测性。每个估计器独立给出一个最小熵估计值，标准规定取其中最小值作为熵源的最小熵（H_original），从而保证估计结果在未知依赖结构下仍然保守可靠。全部估计均在 1,000,000 个样本上执行，是 TRNG 认证中最严格、最常用的一条评估路径。

在室温下，ALEA 设备输出的熵源随机数 non_IID 测试结果如下表所示。

表格 3 non_IID 测试结果（熵源）

Item	Pmax	hmin
MCV	0.50185891	0.994646
Collision	3.3120E-39	0.998652
Markov	0.53062834	0.914226
T-Tuple	0.50351513	0.989893
LRS	0.50136046	0.99608
Multi-MCW	0.50133642	0.996149
Lag	0.50156392	0.995495
Multi-MMC	0.50118842	0.996575
LZ78Y	0.50185891	0.994646

10.3.2 NIST SP 800-22 测试

美国国家标准与技术研究院（NIST）发布的 SP 800-22《A Statistical Test Suite for Random and Pseudo random Number Generators for Cryptographic Applications》（Rev. 1a，2010）是随机数统计检验领域使用最广泛的标准之一。该标准从频数、块内频数、游程、最长游程、矩阵秩、离散傅里叶变换（频谱）、非重叠模板匹配、重叠模板匹配、Maurer 通用统计、线性复杂度、序列相关、近似熵、累加和、随机游走及其变体等多个角度，规定了 15 项统计检验，用于判断二进制序列是否存在偏离随机性的统计特征。检验流程为：对每条被测序列计算 p 值，若 p ≥ α（通常取 0.01）则判定该序列通过；当被测数据包含多条序列时，还需统计通过比例，并对全部 p 值进行均匀性检验（二级 Kolmogorov-Smirnov 检验），只有比例与均匀性同时满足判据，才认为该测试项通过。需要指出的是，统计检验只能发现非随机性，不能证明随机性，因此 SP 800-22 通常与 SP 800-90B、AIS-31 等熵源评估标准配合使用，作为随机数发生器统计质量的常规验证手段。

下表为 SP 800-22 熵源随机数分析典型结果，分析数据个数 1024000。20 组 × 1,024,000 比特的 +20°C 熵源数据 15 项测试全部通过。

表格 4 SP800-22 测试结果（熵源）

测试项	P-VALUE（均匀性）	通过比例	判定
Frequency	0.534146	20/20	Pass
BlockFrequency	0.213309	20/20	Pass
CumulativeSums (1)	0.090936	20/20	Pass
CumulativeSums (2)	0.637119	20/20	Pass
Runs	0.275709	20/20	Pass
LongestRun	0.090936	20/20	Pass

Rank	0.991468	18/20	Pass
FFT	0.066882	20/20	Pass
NonOverlappingTemplate (148)	0.017912~0.991468	114×20/20、30×19/20、4×18/20	Pass
OverlappingTemplate	0.534146	20/20	Pass
Universal	0.066882	20/20	Pass
ApproximateEntropy	0.911413	20/20	Pass
RandomExcursions (8)	0.000648~0.275709	17/17	Pass
RandomExcursionsVariant (18)	0.000060~0.275709	17/17	Pass
Serial (2)	0.534146 / 0.834308	20/20	Pass
LinearComplexity	0.437274	20/20	Pass

10.3.3 Dieharder 测试

Dieharder 是由美国杜克大学 Robert G. Brown 等人开发的开源随机数统计测试套件，在 Marsaglia 的 Diehard 测试集基础上扩展而来，包含经典 Diehard 17 项、RGB 系列以及 STS 系列等 30 余项测试，是目前随机数统计检验中使用最广泛的工具之一。测试时，将待测数据以原始二进制形式（1 字节 8 比特）输入，由 dieharder 逐项读取并计算 p 值：若 p ≥ 0.01，则该测试项判定为 PASSED（通过），否则判定为 FAILED（失败）；当同一测试重复多次时，还会对所得 p 值的均匀性进行进一步检验。本文对 ALEA16 熵源输出数据执行了 dieharder 全部测试，受篇幅限制，正文仅列出经典 Diehard 17 项（test 0~16）的测试结果，RGB 系列、STS 系列等其余测试项的结果从略。

表格 5 Dieharder 测试结果（熵源）

编号	测试名称	p-value	评估
0	diehard_birthdays	0.6889669	PASSED

1	diehard_operm5	0.10689792	PASSED
2	diehard_rank_32x32	0.24253882	PASSED
3	diehard_rank_6x8	0.93919696	PASSED
4	diehard_bitstream	0.91781414	PASSED
5	diehard_opso	0.75276858	PASSED
6	diehard_oqso	0.87287703	PASSED
7	diehard_dna	0.32001859	PASSED
8	diehard_count_1s_str	0.54541444	PASSED
9	diehard_count_1s_byte	0.69708194	PASSED
10	diehard_parking_lot	0.91461926	PASSED
11	diehard_2dsphere	0.97526702	PASSED
12	diehard_3dsphere	0.87881951	PASSED
13	diehard_squeeze	0.02563109	PASSED
14	diehard_sums	0.3200126	PASSED
15	diehard_runs	0.64010050 / 0.34986103	PASSED
16	diehard_craps	0.00837601 / 0.08745911	PASSED

10.3.4 AIS-31 测试

德国联邦信息安全局（BSI）发布的 AIS-31《Functionality Classes for Random Number Generators》是另一套被广泛采用的随机数评估标准，与 NIST SP 800-90B 互为补充。AIS-31 将随机数发生器划分为 PTG.2、PTG.3（物理真随机）和 DRG（确定性）等功能类，并规定了一套统计检验流程：T0 不相交性检验、T1 单比特检验、T2 扑克检验、T3 游程检验、T4 长游程检验、T5 自相关检验、T6 均匀分布检验、T7 多项分布检验和 T8 熵检验。其中 T1T8 在更大样本上执行，用于评估分布均匀性与熵水平。所有检验须同时满足标准规定的上下界，才能判定该熵源通过 AIS-31 评估。

下表为 AIS-31 熵源随机数分析典型结果，分析数据个数 1E6。所有测试均通

过。

表格 6 AIS-31 测试项和结果（熵源）

AIS-31	Test Result
Disjointness Test (TO)	PASS
Monobit Tests (T1)	PASS
Poker Tests (T2)	PASS
Run Tests (T3)	PASS
Long Run Test (T4)	PASS
Autocorrelation Test (T5)	PASS
Uniform Distribution Test (T6)	PASS
Multinomial Distributions (T7)	PASS
Entropy Test (T8)	PASS

10.3.5 分布均一性测试

理想情况下，TRNG 产生 0 和 1 的概率应当完全相同。序列偏置会削弱随机性，并使 TRNG 易受攻击。我们用下式评估随机序列的偏置大小：

$$Bias = \frac{|N_1 - N_2|}{N_1 + N_2} \times 100\%$$

其中 N1 和 N2 分别为比特 1 和比特 0 的个数。实测的统计偏差为 0.029%。

随机比特流还被转换为二维比特流图像，如下图所示。在左图中，比特 1 渲染为黑色像素，而在右图中则用白色像素表示。黑白像素分布均匀，验证了所生成的随机数具有均匀性和低偏置。

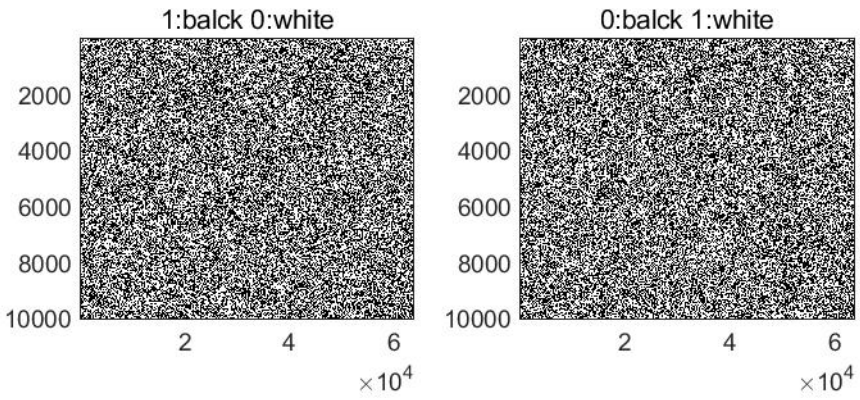

图 1 比特 0 和 1 二维分布图 9（熵源）

10.3.6 温度漂移测试

10.3.6.1 测试平台

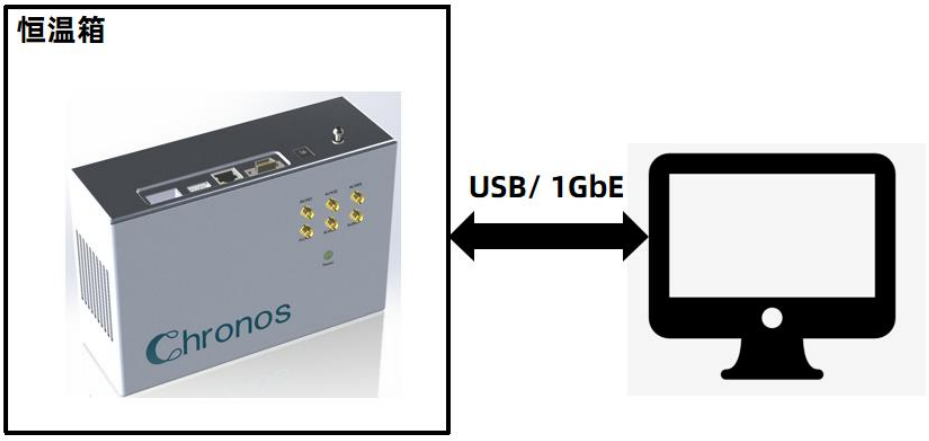

图 2 温漂测试平台示意图

为评估温度对随机数发生器性能的影响，搭建了如图所示的温漂测试平台。平台由恒温箱、ALEA 随机数发生器样机和上位机三部分组成：样机置于恒温箱内，通过 USB 3.0 或 1 GbE 接口与箱外上位机连接，实现随机数数据的实时采集与存储。测试时，将恒温箱分别设定为 −10 °C、0 °C、+10 °C、+20 °C、+30 °C 和 +40 °C 六个温度点，待箱内温度稳定并使样机充分热平衡后，由上位机连续采集原始熵源比特流与 SM3 调理后的输出比特流，每组数据保存为独立的二进

制文件；随后使用 NIST SP 800-90B 参考工具（ea_iid 与 ea_non_iid）对两组数据分别进行 IID 与非 IID 分析，得到各温度点下的最小熵估计值。样机的 FPGA 内核温度可通过片上 XADC 实时读取，用于记录环境温度与芯片结温的对应关系。

10.3.6.2 IID 测试

NIST SP 800-90B IID 测试评估随机性温漂。测试结果如下表所示，每次测试分析数据个数 1E6。

表格 7 IID 温漂测试结果（熵源）

环境温度(℃)	FPGA 核心温度(℃)	Raw Mean	MCV p_u	H_original	Chi2 ind p	Chi2 GOF p
-10	30	0.499823	0.50146492	0.995779	0.621915	0.490764
0	38	0.498922	0.50236591	0.993190	0.082079	0.752949
+10	46	0.500869	0.50215691	0.993790	0.229684	0.802009
+20	55	0.499429	0.50185891	0.994646	0.133522	0.690442
+30	60	0.499959	0.50132892	0.996171	0.708690	0.254620
+40	68	0.500166	0.50145392	0.995811	0.026492	0.189058

最小熵与外界环境温度的关系如下图所示。

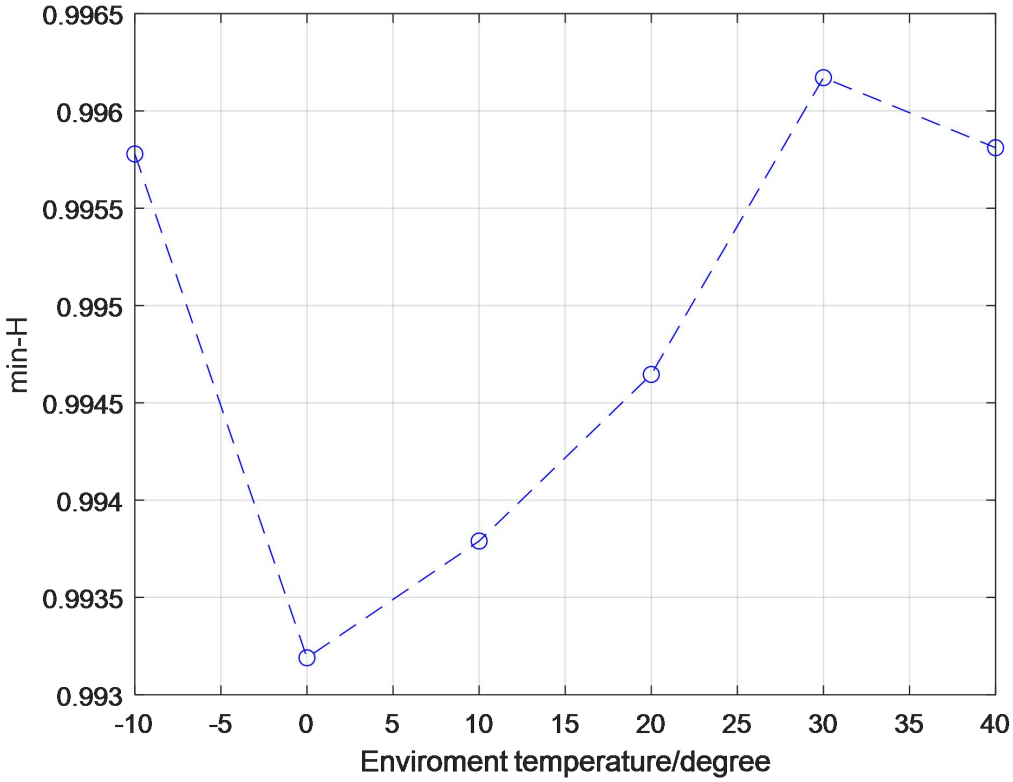

图 3 IID 最小熵与环境温度测试结果（熵源）

10.3.6.2 non_IID 测试

NIST SP 800-90B non_IID 熵源测试评估随机性温漂。测试结果如下表所示，每次测试分析数据个数 1E6。

表格 8 NIST SP 800-90B 温漂测试结果（熵源）

温度(°C)	FPGA 核心温度(°C)	MCV	Collision	Markov	T-Tuple	LRS	Multi-MCW	Lag	Multi-MMC	LZ78Y
-10	30	0.995779	0.934754	0.997759	0.94154	0.976287	0.99692	0.995646	0.997167	0.995436
0	38	0.99319	0.917854	0.997036	0.919089	0.994334	0.99635	0.994777	0.995161	0.993694
10	46	0.99379	0.947521	0.997728	0.921623	0.994988	0.997767	0.998052	0.995555	0.996981
20	55	0.994646	0.914499	0.998652	0.914226	0.989893	0.99608	0.996149	0.995495	0.996575
30	60	0.996171	0.913806	0.99884	0.921623	0.977339	0.996514	0.996699	0.994396	0.99773
40	68	0.995811	0.944247	0.99896	0.93978	0.99063	0.994762	0.995507	0.995345	0.996345

10.3.7 重启测试

ALEA 设备经过 1000 次上电重启，采集超过 1E6 个随机数序列，测试 NIST SP 800-90B IID，其最小熵均大于 0.99 bit。

10.4 SM3 输出测试

10.4.1 NIST SP 800-90B 测试

10.4.1.1 IID 测试

在室温下，ALEA 设备输出的随机数 IID 测试结果如下表所示。最小熵为 0.996243 bit。

表格 9 IID 测试结果

参数	值	说明
样本数	1000000	
Raw Mean	0.500016	原始均值
Median	0.5	中位数
Binary	TRUE	二值数据
MCV mode	500016	最常见值出现次数
MCV p-hat	0.500016	最常见值概率
MCV p_u	0.50130392	99% 上界
MCV H_original	0.996243	IID 轨最小熵
Chi-square independence score	1984.019318	独立性卡方统计量
Chi-square independence dof	2046	自由度
Chi-square independence p-value	0.833586	>0.01 通过
Chi-square goodness score	8.780496	拟合优度统计量
Chi-square goodness dof	9	自由度
Chi-square goodness p-value	0.457778	>0.01 通过
Chi-square tests	0.5	卡方测试结论
LRS P_col	38	最长重复子串 P_col
LRS Length	0.837788	最长重复子串长度
LRS Pr(X>=1)	19/19	LRS 概率
LRS test	Passed	LRS 结论
Permutation tests	1000000	置换检验结论
Overall IID	0.500016	总体结论

10.4.1.2 non_IID 测试

下表为 NIST SP 800-90B non_IID 随机数分析典型结果，分析数据个数 1E6。

表格 10 NIST SP 800-90B 测试结果

Item	Pmax	hmin
MCV	0.50130392	0.996243
Collision	3.4751E-39	0.99811
Markov	0.52884286	0.919089
T-Tuple	0.50248909	0.992836
LRS	0.50092743	0.997326
Multi-MCW	0.50105642	0.996955
Lag	0.50096392	0.997221
Multi-MMC	0.50155443	0.995522
LZ78Y	0.50130392	0.996243

10.4.2 NIST SP 800-22 测试

下表为 SP 800-22 随机数分析典型结果，分析数据个数 1024000。20 组 × 1,024,000 比特的 +20℃ 熵源数据 15 项测试全部通过。

表格 11 SP800-22 测试结果

测试项	P-VALUE（均匀性）	通过比例	判定
Frequency	0.437274	20/20	Pass
BlockFrequency	0.637119	20/20	Pass
CumulativeSums (1)	0.162606	20/20	Pass
CumulativeSums (2)	0.162606	20/20	Pass
Runs	0.122325	20/20	Pass
LongestRun	0.911413	20/20	Pass
Rank	0.048716	20/20	Pass
FFT	0.911413	20/20	Pass
NonOverlappingTemplate (148)	0.006196~1.000000	18/20×4; 19/20×19; 20/20×125	Pass
OverlappingTemplate	0.437274	20/20	Pass
Universal	0.035174	20/20	Pass

ApproximateEntropy	0.534146	20/20	Pass
RandomExcursions (8)	0.001399~0.275709	17/17	Pass
RandomExcursionsVariant (18)	0.000005~0.437274	16/17×1; 17/17×17	Pass
Serial (2)	0.739918	20/20	Pass
LinearComplexity	0.834308	20/20	Pass

10.4.3 Dieharder 测试

本文对 ALEA16 熵源输出数据执行了 dieharder 全部测试，受篇幅限制，正文仅列出经典 Diehard 17 项（test 0~16）的测试结果，RGB 系列、STS 系列等其余测试项的结果从略。

表格 12 Dieharder 测试结果

编号	测试名称	p-value	评估
0	diehard_birthdays	0.54571716	PASSED
1	diehard_operm5	0.01692343	PASSED
2	diehard_rank_32x32	0.8719463	PASSED
3	diehard_rank_6x8	0.72873507	PASSED
4	diehard_bitstream	0.95568182	PASSED
5	diehard_opso	0.20530157	PASSED
6	diehard_oqso	0.61183805	PASSED
7	diehard_dna	0.07019509	PASSED
8	diehard_count_1s_str	0.50886925	PASSED
9	diehard_count_1s_byte	0.00324662	WEAK
10	diehard_parking_lot	0.77995133	PASSED
11	diehard_2dsphere	0.9225098	PASSED
12	diehard_3dsphere	0.23210984	PASSED
13	diehard_squeeze	0.15506921	PASSED
14	diehard_sums	0.91045352	PASSED
15	diehard_runs	0.15470826 / 0.33694933	PASSED
16	diehard_craps	0.04814346 / 0.00127811	PASSED

10.4.4 AIS-31 测试

下表为 AIS-31 熵源随机数分析典型结果，分析数据个数 1E6。所有测试均通过。

表格 13 AIS-31 测试项和结果

AIS-31	Test Result
Disjointness Test (TO)	PASS
Monobit Tests (T1)	PASS
Poker Tests (T2)	PASS
Run Tests (T3)	PASS
Long Run Test (T4)	PASS
Autocorrelation Test (T5)	PASS
Uniform Distribution Test (T6)	PASS
Multinomial Distributions (T7)	PASS
Entropy Test (T8)	PASS

10.4.5 分布均一性测试

随机比特流还被转换为二维比特流图像，如下图所示。在左图中，比特 1 渲染为黑色像素，而在右图中则用白色像素表示。黑白像素分布均匀，验证了所生成的随机数具有均匀性和低偏置（~0.004%）。

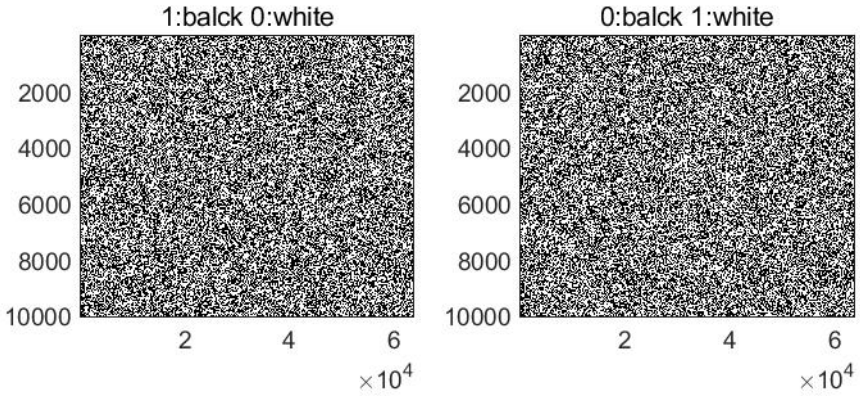

图 4 比特 0 和 1 二维分布图

10.4.6 温度漂移测试

10.4.6.1 IID 测试

NIST SP 800-90B IID 测试评估随机性温漂。测试结果如下表所示，每次测试分析数据个数 1E6。

表格 14 IID 温漂测试结果

环境温度(℃)	FPGA 核心温度(℃)	Raw Mean	MCV p_u	H_original	Chi2 ind p	Chi2 GOF p
-10	30	0.499912	0.50137592	0.996035	0.519221	0.611226
0	38	0.500567	0.50185491	0.994658	0.158117	0.96485
+10	46	0.499838	0.50144992	0.995822	0.307809	0.618412
+20	55	0.500016	0.50130392	0.996243	0.833586	0.457778
+30	60	0.49992	0.50136792	0.996058	0.556855	0.671757
+40	68	0.500027	0.50131492	0.996211	0.414055	0.216959

最小熵与外界环境温度的关系如下图所示。

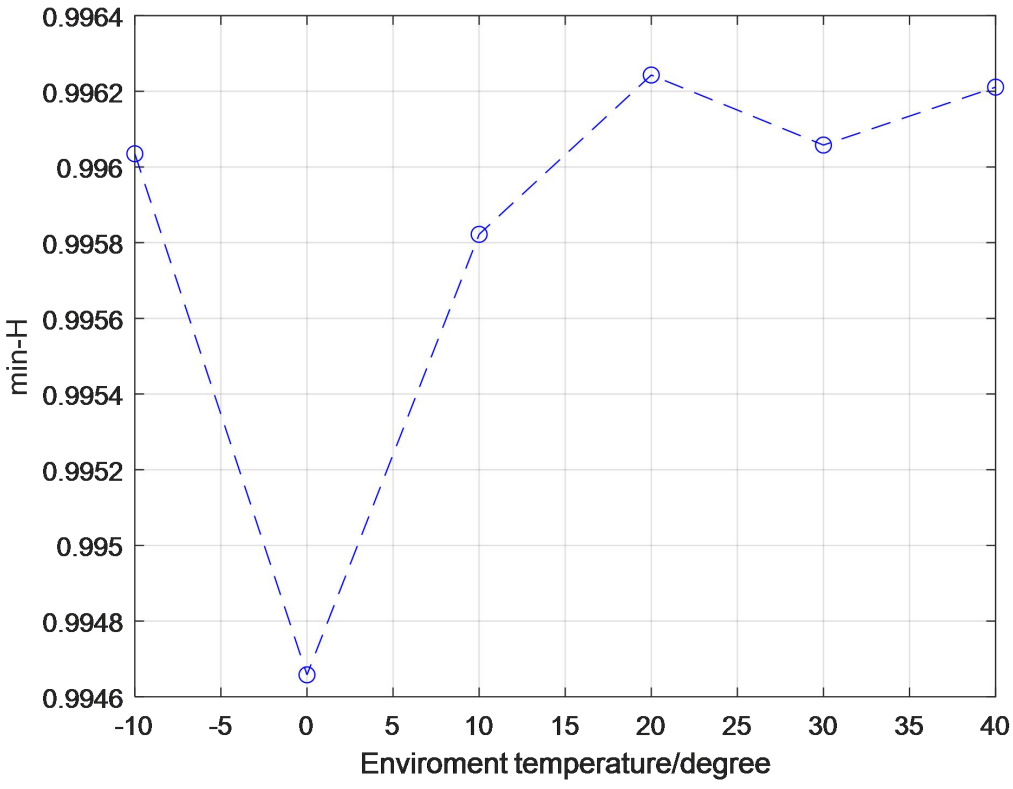

图 5 IID 最小熵与环境温度测试结果

10.4.6.1 non_IID 测试

NIST SP 800-90B non_IID 测试评估随机性温漂。测试结果如下表所示，每次测试分析数据个数 1E6。

表格 15 NIST SP 800-90B 温漂测试结果

温度(°C)	FPGA 核心温度(°C)	MCV	Collision	Markov	T-Tuple	LRS	Multi-MCW	Lag	Multi-MMC	LZ78Y
-10	30	0.996035	0.926452	0.999769	0.93978	0.970832	0.996912	0.996592	0.99615	0.996915
0	38	0.994658	0.88959	0.99634	0.921623	0.994165	0.995775	0.996267	0.995023	0.996011
10	46	0.995822	0.891818	0.998117	0.921623	0.987786	0.99633	0.998883	0.996081	0.996995
20	55	0.996243	0.90184	0.99811	0.919089	0.992836	0.997326	0.996955	0.997221	0.995522
30	60	0.996058	0.914083	0.998505	0.936354	0.996326	0.995959	0.996995	0.997339	0.99894
40	68	0.996211	0.879668	0.997617	0.914226	0.996096	0.995712	0.998444	0.994939	0.995217

10.4.7 重启测试

- ALEA 设备经过 1000 次上电重启，采集超过 1E6 个随机数序列，分析其 NIST SP 800-90B IID 测试，其最小熵均大于 0.99 bit。

本文档历史记录

文档编号	修改时间	修改人	说明
UG-03-1-010-1	2026.11	Cong	V1.0