SP800-90B Non-Proprietary Public Use Document

Quantis QRNG IID Chips

IDQ250C2, IDQ250C3, IDQ6MC1, IDQ20MC1, IDQ20MC1-S1, IDQ20MC1-S3

Version 0.4

Date: 20/07/23

Document History

Version	Date (mm/dd/yyyy)	By	Changes
0.1	16/12/2022	Kevin LAYAT	First version
0.2	20/12/2022	Kevin LAYAT	Format document to match PUD requirements
0.3	23/03/2023	Kevin LAYAT	Match CMVP Template
0.4	20/07/2023	Kevin LAYAT	Comments answers

Table of contents

Figures

Tables

List of Acronyms and Glossaries

Acronyms	Descriptions
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standard
NIST SP	National Institute of Standards and Technology Special Publication
NRBG	Non-deterministic Random Bit Generator
QRNG/TRNG/PRNG	Quantum/True/Pseudo Random Number Generator
SPI	Serial Peripheral Interface
I2C	Inter-Integrated Circuit
APT	Adaptive Proportion Test
RCT	Repetition Count Test
IID	Independent and Identically Distributed
LED	Light Emitting Diode
LDO	Low Voltage Dropout
CIS	CMOS Image Sensor
ADC	Analog Digital Converter
ASIC	Application Specific Integrated Circuit
PCB	Printed Circuit Board
FPGA	Field Programmable Gate Array
CAVP	Cryptographic Algorithm Validation Program

1. Description

Quantis IDQ250C2, IDQ250C3, IDQ6MC1, IDQ20MC1, IDQ20MC1-S1 and IDQ20MC1-S3 chips are based on a physical noise source (P) that meets the requirements of NIST SP 800-90B. The IID entropy estimation track is chosen. Independent, meaning the sample items are all independent events and not connected to each other, and Identically Distributed, meaning there are no overall trends and all items in the sample are taken from the same probability distribution, is the ideal track for randomness.

To get high quality of entropy, IDQ's patented QRNG chips exploit the fact that the number of photons emitted by a common light source fluctuates randomly. These fluctuations, also called "quantum shot noise", are purely of a quantum origin, and are therefore fundamentally random as per the laws of physics: an array of single-photon sensitive pixels is illuminated for a short time during which each pixel receives a random number of incident photons that follows the statistics of a Poisson distribution.

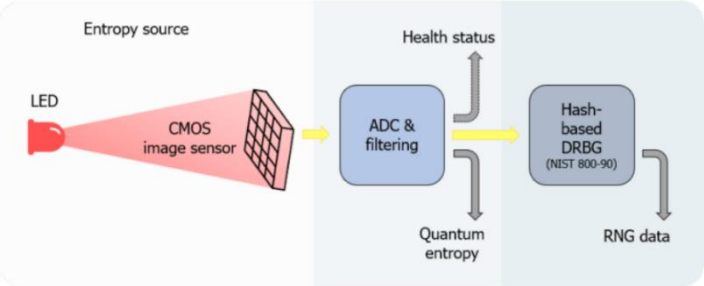

Figure 1: Basic structure for IDQ IID QRNG chips

IDQ IID QRNG chips basically follow the structure in to generate entropy bits: a light emitting diode (LED) and a CMOS image sensor (CIS) pixel array are respectively integrated inside a QRNG chip as a light source and a multipixel photon detector. All pixel outputs are digitized by a single analog-digital converter (ADC). Based on these ADC output values, the number of detected photons per pixel, as well as their fluctuations, can be measured. Essentially, the quantum shot noise is directly converted into numbers at the output of the ADC. The passage from quantum randomness to an actual random number is straight forward and by no means affected by other unaccounted (and possibly contriving) physical processes that could increase predictability and thwart security.

IDQ provides six types of QRNG chips, IDQ250C2, IDQ250C3, IDQ6MC1 IDQ20MC1, IDQ20MC1-S1 and IDQ20MC1-S3 which generate unpredictable entropy bits based on quantum randomness. As shown in Table 1 and Table 2, they are all compliant to the NIST SP 800-90B, which stipulate the security requirements for the FIPS-approved entropy sources.

Model	IDQ20MC1-S1	IDQ20MC1-S3
Quantum Entropy data rate	20 Mb/s	20 Mb/s
Small size	4.2 x 5 x 1.1 mm	4.2 x 5 x 1.1 mm
Simple and easy to integrate (standard SPI interface)	SPI	SPI
Live status verification and Health check output	✓	✓
Integrated NIST 800-90 A/B/C compliant DRBG post-processing	✓	✓
Robust to harsh space conditions	Class 1	Class 3
Works with traditional encryption algorithms and PQC	✓	✓

Table 1: Specification of IDQ IID QRNGs for space

Model	IDQ250C3	IDQ250C2	IDQ6MC1	IDQ20MC1
QRNG CORE				
Compliant to the Standard NIST 800-90A/B/C	✓ (B)	✓ (B)	✓	✓
Certified AEC-Q100			✓	
Size	3 x 3 x 0.8 mm	2.5 x 2.5 x 0.84 mm	4.2 x 5 x 1.1 mm	4.2 x 5 x 1.1 mm
RNG Data Output	N/A	N/A	1.47 Mbps (@ SPI Interface)	4.90 Mbps
Quantum Entropy Source	250 Kbps (typical)	250 Kbps (typical)	5.88 Mbps (@ SPI Interface)	19.64 Mbps
POWER SUPPLY INFORMATION				
Single Input Voltage (Embedded LDO)	2.8V	2.8V	2.8V	2.8V
I/O Interface Voltage	1.8V	1.8V	1.8V	1.8V
POWER CONSUMPTION				
RNG Output Mode	N/A	N/A	59.94 mW	83.44 mW
Entropy Output (sample mode)	15 mW (typical)	15 mW (typical)	58.24 mW	75.88 mW
Power Down Mode	100 uW	100 uW	N/A	N/A
SET-UP TIME				
Initial set-up time	3 ms	3 ms	171 ms	184 ms
OPERATION FREQUENCY CLOCK & TEMPERATURE				
Embedded ROSC	11 MHz ~ 14 MHz (Typ. 12 MHz)	11 MHz ~ 14 MHz (Typ. 12 MHz)	41 MHz ~ 58 MHz (Typ. 48 MHz)	41 MHz ~ 58 MHz (Typ. 48 MHz)
Recommended temperature	-20 °C ~ +85 °C	-20 °C ~ +85 °C	-20 °C ~ +85 °C	-30 °C ~ +85 °C
Absolute maximum rated temperature	-40 °C ~ +105 °C	-40 °C ~ +105 °C	-40 °C ~ +105 °C	-40 °C ~ +105 °C
INTERFACE PROTOCOL				
SPI			24 MHz	24 MHz x 4 CH
I2C	400 KHz	400 KHz	100 KHz	

Table 2: Specification of IDQ IID QRNGs

2. Security Boundary

The physical and logical security boundaries of IDQ IID QRNG chips are limited to and fully depend on those of the host security devices integrating IDQ IID QRNG chips inside. IDQ IID QRNG chips are not a stand-alone security module but rather play a role of an embedded sub-component feeding physical entropy bits to a host device within its security boundary. IDQ IID QRNG chips are composed of a physical chipset and a host driver software, which are connected by SPI or I2C. All the chip, host driver, and physical/logical paths between them shall be securely protected and controlled by the physical protection mechanism and the security policy of the host device.

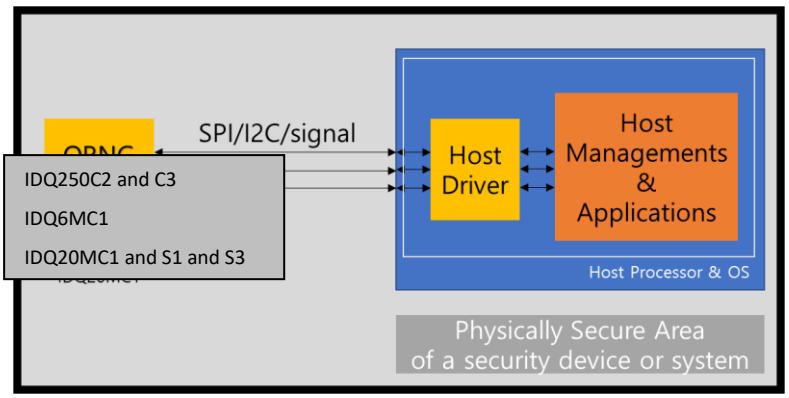

Figure 2: Boundary for IDQ IID QRNG chip and its host driver

3. Operating Conditions

As a semi-conductor product, the reliability of the IDQ IID QRNG chips has been certified in various environmental situations, by the standards such as EMI/EMC, AEC-Q100, and so on. Based on them, the actual operating conditions for temperature and voltage are set as follows:

- Temperature Range for IDQ20MC1, S1 and S3:
  - Recommended: -30℃ to 85℃
  - Absolute Maximum Rated Temperature: -40℃ to 105℃
  - Storage Temperature: -40℃ to 125℃
- Temperature Range for IDQ6MC1, IDQ250C2 and C3
  - Recommended: -20℃ to 85℃
  - Absolute Maximum Rated Temperature: -40℃ to 105℃
  - Storage Temperature: -40℃ to 125℃
- Input Voltage for all chips (acceptable by the LDO): 2.8V ± 15%

4. Configuration Settings

IDQ IID QRNG chips only take the responsibility on the ESV part. The security levels should be determined depending on how host devices operate and manage our QRNG chips. Although IDQ provides a host driver associated to the type of QRNG chip, the host driver should be treated as a reference. Users can modify the host driver with full degree of freedom on their needs unless the modifications do make any effect on the security. Currently, the host driver supports Linux OS environments and users can register it either as /dev/hwrng for the Linux kernel or as a character device easily handled from user applications.

The interfaces of the chips are only for internal use, the access to which should be securely controlled by the host device's security policy, and moreover the extracted entropy data should be treated as a critical security parameter. It is recommended to extract the entropy bits newly only when needed and only as many as needed. The memory space in the host device containing the entropy bits should be accessible only by the authorized users or processes and, if possible, zeroized whenever an attack or unauthorized access is detected. The host drivers for running IDQ IID QRNG chips must be considered as a part of the software package of the host device and thus the program itself should be also securely operated in the host device's security policy during the whole lifetime at boot and at operation.

The logic designs of QRNG chips are hard coded by electronic circuits and there is no possibility to change them after the production. Vendors can have a chance in theory to adjust and optimize some register parameters of the QRNG chip during developments. However, this modification shall be confirmed by IDQ and after finishing the optimization, nothing shall be changed.

5. Min-Entropy Rate

IDQ IID QRNG chips guarantee the min-entropy per 2-bit sample of at least over 1.90, which is obtained by the theoretical analysis based on the physical model of our QRNG chips. Under the IID claim, the NIST IID test tool gives pass results and higher score on the min-entropy estimation than our theoretical analysis result, 1.90 (IID and restart test included). Of course, the non-IID entropy estimation (conservative choice because more pessimistic than IID), are also giving good results, the min-entropy per 2-bit sample is always more than 1.75 as shown in the Table 3.

	IDQ250C2	IDQ250C3	IDQ6MC1	IDQ20MC1
H_submitter	1.75	1.75	1.75	1.75
H=min(H_r, H_c, H_i)	1.810845	1.760755	1.807423	1.827089
Bits per request	2	2	2	2

Table 3: Min-Entropy rate summary

6. Conceptual Interfaces

According to the model of IDQ IID QRNG chip, different types of interfaces are given to users.

1) Entropy interface of IDQ250C2 and C3
   A. IDQ250C2 and C3 only provides raw entropy bits directly extracted from the physical entropy source. There is no DRBG mechanism inside IDQ250C2 and C3.
   B. Through the interface, it is possible to get not only raw entropy bits but also the chip's internal information such as the health status of physical components and the readiness for entropy data transmission. Especially the health status is given in every data packet together with raw entropy bits for real-time health check.
   C. In addition, the NIST statistical health tests are performed in the host driver.
2) Entropy interface of IDQ6MC1 and IDQ20MC1s
   A. IDQ6MC1 and IDQ20MC1s also support two types of interfaces, Entropy and RNG. In fact, they are designed to satisfy all the requirements of the NIST SP 800-90A, B and C. The RNG interface outputs the random bits which is generated by applying the hash-based

DRBG mechanism to the raw entropy bits based on the oversampling enhanced-NRBG construction. However, this interface is out of scope as mentioned before.

B. Users can obtain raw entropy bits from the Entropy interface. However, unlike IDQ250C2 and C3, the Entropy interface does not provide the physical health status information. Therefore, the health check on the entropy bits fully depends on the NIST statistical health tests in the host driver.

7. Analog Calibration and Health Test

Power-up Calibration Sequence and Continuous Health Check

After the initialization of MCU and CIS sensor is done, the chip checks out the CIS's dark noise level and the LED status. Then the light brightness level of LED is automatically calibrated, and the pixel outputs are sustained in the middle of the ADC output range without saturating to the min and the max values.

During the operation, it is counted every frame how many pixels are beyond the min or max threshold. If the number corresponding to either the min or the max threshold is greater than or equal to 10, then the entropy generation is stopped, and the recalibration is activated in the same way to the initialization. If the failure happens two times consecutively, then it is considered as a total failure and the chip is permanently stopped.

Health Check

Several health checks are performed during the lifecycle of the devices:

- **Start-up Test:** Whenever 'start' or 'restart' happens, QRNG chip runs the start-up test (operating on bytes) over 1,024 bytes of entropy composed of 4096 2-bits samples (concatenated into bytes). If there happens a failure, then the host driver stops working and returns the failure. Then users should decide whether to retry or not according to their security policy.

- **Continuous Test:** After the start-up test is passed, RCT and APT (operating on bytes) are running over all entropy outputs continuously as defined in the NIST SP 800-90B. In this setting, we treat one failure in RCT or APT as normal or temporary one and raise an alarm only when more than two failures in either RCT or APT happen within 10 tests.
- **Final Failure Probability:** The final failure alarm is given only when either RCT or APT face more than 2 failures within 10 tests.

8. Required Testing

The tests below show the results of running the NIST entropy assessment. Statistical testing was performed across the expected operational temperature range of the device to demonstrate the noise source's performance does not degrade. The physical construction of the noise source does not allow for any other testing methodology to be done.

Raw Data Collection

The testing in the following section has been performed in accordance with Section 3.1 and 3.2 of NIST SP 800-90B. All samples have been obtained directly from the noise source through the raw noise source interface and are considered "raw data".

Samples were collected by running the chip in "raw mode". Once the required number of samples was collected, non-restart and restart testing files were used as input into the NIST entropy assessment tool. The "raw mode" is available for all the chip versions, for IDQ250C2 and IDQ250C3 it is the only available mode, which means a user can reproduce the following test with any output of these chips to control the correct behavior of a device. For IDQ6MC1 and the IDQ20MC1 suite, two modes are available; the "RNG mode" (which a apply a NIST compliant DRBG mechanism) and the "raw mode" that can again be used to reproduce the following tests. A user may then be able to configure the device in the correct mode to directly access the raw data. The mode selection and data access can be done using a specific software (driver) provided by ID Quantique.

The entropy rate must be at least the min-entropy rate as defined in the Min-Entropy Rate Section.

Test Results for IID assessment

The testing methodology follows the report of the NIST entropy assessment test on 10,000,000 2-bit samples produced by the chip. The summary tables includes random data collected in different temperatures mentioned in the section *Operating Conditions*.

Value	-20°C	-10°C	0°C	15°C	30°C	45°C	60°C	75°C	85°C
$H_{original}$	7.927324	7.922211	7.924899	7.921103	7.924227	7.931745	7.940867	7.940663	7.936926
$H_{bitstring}$	0.997656	0.992157	0.994902	0.992295	0.993202	0.994542	0.992919	0.994518	0.994882
$\min(H_o, 8xH_b)$	1.983022	1.982677	1.983224	1.982672	1.982799	1.986944	1.985317	1.987874	1.988593

Table 4: Summary of IID random tests for IDQ250C2

The lowest value for IDQ250C2 of the min ($H_{original}$, 2 x $H_{bitstring}$) is 1.982672 which occurs at 15°C.

Value	-20°C	-10°C	0°C	15°C	30°C	45°C	60°C	75°C	85°C
$H_{original}$	1.975827	1.969534	1.973805	1.970796	1.973045	1.976388	1.978346	1.980389	1.979199
$H_{bitstring}$	0.987095	0.984796	0.984307	0.987711	0.989760	0.991397	0.992824	0.993682	0.994523
$min(H_o, 8xH_b)$	1.974191	1.969534	1.968613	1.970796	1.973045	1.976388	1.978346	1.980389	1.979199

Table 5: Summary of IID random tests for IDQ250C3

The lowest value for IDQ250MC3 of the min ($H_{original}$, 2 x $H_{bitstring}$) is 1.968613 which occurs at 0°C.

Value	-20°C	-10°C	0°C	15°C	30°C	45°C	60°C	75°C	85°C
$H_{original}$	1.987567	1.990014	1.990195	1.994425	1.991411	1.992980	1.992477	1.994406	1.996238
$H_{bitstring}$	0.995972	0.996885	0.996884	0.998197	0.996842	0.997543	0.997395	0.998250	0.998801
$min(H_o, 8xH_b)$	1.987567	1.990014	1.990195	1.994425	1.991411	1.992980	1.992477	1.994406	1.996238

Table 6: Summary of IID random tests for IDQ6MC1

The lowest value for IDQ6MC1 of the min ($H_{original}$, 2 x $H_{bitstring}$) is 1.987567 which occurs at -20°C.

Value	**-30°C**	-20°C	-10°C	0°C	15°C	30°C	45°C	60°C	75°C	85°C
$H_{original}$	1.987387	1.992262	1.993730	1.995207	1.997129	1.997008	1.996198	1.995673	1.995011	1.993830
$H_{bitstring}$	0.996685	0.998011	0.998230	0.998540	0.999063	0.999114	0.998661	0.998996	0.998825	0.999092
$min(H_o, 8xH_b)$	1.987387	1.992262	1.993730	1.995207	1.997129	1.997008	1.996198	1.995673	1.995011	1.993830

Table 7: Summary of IID random tests for IDQ20MC1

The lowest value for IDQ20MC1 of the min ($H_{original}$, 2 x $H_{bitstring}$) is 1.987387 which occurs at -30°C.

The results show that the entropy data produced by the chip are always in the required range and that the entropy quality produced by the chip is not affected by the change in working environment. Snip of raw data tests for IDQ250C3 at 0°C:

```
Opening file: 'IDQ250C3_at0_iid.bin'
Loaded 10485760 samples of 4 distinct 2-bit-wide symbols
```

```
Number of Binary samples: 20971520
Calculating baseline statistics...
       Raw Mean: 1.515626
       Median: 2.000000
       Binary: false

Literal MCV Estimate: mode = 2665841, p-hat = 0.25423440933227537, p_u =
0.25458077551170366
Bitstring MCV Estimate: mode = 10594548, p-hat = 0.50518741607666018, p_u =
0.50546863773533879
H_original: 1.973805
H_bitstring: 0.984307
min(H_original, 2 X H_bitstring): 1.968613
Chi square independence
       score = 103.562697
       degrees of freedom = 12
       p-value = 0.000000

** Failed chi square tests

Literal Longest Repeated Substring results
       P_col: 0.250123
       Length of LRS: 22
       Pr(X >= 1): 0.957536
** Passed length of longest repeated substring test

Beginning initial tests...

Initial test results
              excursion: 5942.37
     numDirectionalRuns: 6.55464e+06
     lenDirectionalRuns: 16
  numIncreasesDecreases: 6.55235e+06
          numRunsMedian: 5.24191e+06
          lenRunsMedian: 23
           avgCollision: 3.21812
           maxCollision: 5
         periodicity(1): 2.62175e+06
         periodicity(2): 2.62224e+06
         periodicity(8): 2.62228e+06
        periodicity(16): 2.62068e+06
        periodicity(32): 2.6218e+06
```

```
          covariance(1): 2.4088e+07
          covariance(2): 2.40868e+07
          covariance(8): 2.40906e+07
         covariance(16): 2.408e+07
         covariance(32): 2.40866e+07
            compression: 2.82451e+06
                statistic  C[i][0]  C[i][1]  C[i][2]
-----------------------------------------------------
                excursion        6        0      976
       numDirectionalRuns        6        0       86
       lenDirectionalRuns        2        4        6
    numIncreasesDecreases      565        0        6
            numRunsMedian        8        0        6
            lenRunsMedian        5        2        4
             avgCollision       16        0        6
             maxCollision        0        6        0
           periodicity(1)       29        0        6
           periodicity(2)       12        0        6
           periodicity(8)        6        0        6
          periodicity(16)       57        0        6
          periodicity(32)       12        0        6
            covariance(1)        6        0       10
            covariance(2)        6        0       11
            covariance(8)        6        0       34
           covariance(16)       95        0        6
           covariance(32)        8        0        6
              compression        6        0       10
(* denotes failed test)

** Passed IID permutation tests
```

Test Results for restart test

The restart process simulates the real-world process specified in SP800-90B and is composed of series of chip restart (1000 restarts) and at each restart 1000 2-bit samples of entropy are collected. The restart sanity tests must all pass, and the minimum of the row-wise and column-wise entropy rate should not be less than half of the entropy rate obtained from the raw noise data test.

The summary table includes restart data collected in different temperatures.

Value	-20°C	-10°C	0°C	15°C	30°C	45°C	60°C	75°C	85°C
X_{cutoff}	319	319	319	318	319	317	317	317	318
X_{max}	306	301	303	302	309	302	297	302	301
RST results	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
H_r	1.979897	1.980405	1.979755	1.978604	1.978741	1.985488	1.981112	1.986690	1.985419
H_c	1.979897	1.980405	1.979755	1.978604	1.978741	1.985488	1.981112	1.986690	1.985419
H_I	1.983022	1.982677	1.983224	1.982672	1.982799	1.986944	1.985317	1.987874	1.988593
$H=\min(H_r, H_c, H_I)$	1.979897	1.980405	1.979755	1.978604	1.978741	1.985488	1.981112	1.986690	1.985419

Table 8: Summary of IID restart tests for IDQ250C2

The lowest value for IDQ250C2 of H is 1.978604 which occurs at 15°C.

Value	-20°C	-10°C	0°C	15°C	30°C	45°C	60°C	75°C	85°C
X_{cutoff}	320	320	321	320	320	319	319	319	318
X_{max}	308	312	300	300	309	306	302	305	307
RST results	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
H_r	1.971521	1.961757	1.967340	1.969505	1.971810	1.971447	1.974669	1.974260	1.980382
H_c	1.971521	1.961757	1.967340	1.969505	1.971810	1.971447	1.974669	1.974260	1.980382
H_I	1.974191	1.969534	1.968613	1.970796	1.973045	1.976388	1.978346	1.980389	1.979199
$H=\min(H_r, H_c, H_I)$	1.971521	1.961757	1.967340	1.969505	1.971810	1.971447	1.974669	1.974260	1.979199

Table 9: Summary of IID restart tests for IDQ250C3

The lowest value for IDQ250C3 of H is 1.961757 which occurs at -10°C.

Value	-20°C	-10°C	0°C	15°C	30°C	45°C	60°C	75°C	85°C
X_{cutoff}	317	317	317	316	318	318	315	317	316
X_{max}	301	299	302	304	300	303	301	313	311
RST results	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
H_r	1.984939	1.985413	1.983601	1.981477	1.989212	1.991221	1.990382	1.988432	1.988357
H_c	1.984939	1.985413	1.983601	1.981477	1.989212	1.991221	1.990382	1.988432	1.988357
H_l	1.987567	1.990014	1.990195	1.994425	1.991411	1.992980	1.992477	1.994406	1.996238
$H=min(H_r, H_c, H_l)$	1.984939	1.985413	1.983601	1.981477	1.989212	1.991221	1.990382	1.988432	1.988357

Table 10: Summary of IID restart tests for IDQ6MC1

The lowest value for IDQ6MC1 of H is 1.981477 which occurs at 15°C

Value	-30°C	-20°C	-10°C	0°C	15°C	30°C	45°C	60°C	75°C	85°C
X_{cutoff}	318	317	316	316	317	316	316	316	316	316
X_{max}	299	306	300	301	298	308	298	303	299	302
Rst Sanity Check	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
H_r	1.981916	1.989040	1.986747	1.987881	1.991376	1.992376	1.991991	1.989567	1.989510	1.989022
H_c	1.981916	1.989040	1.986747	1.987881	1.991376	1.992376	1.991991	1.989567	1.989510	1.989022
H_l	1.987387	1.992262	1.993730	1.995207	1.997129	1.997008	1.996198	1.995673	1.995011	1.993830
$H=min(H_r, H_c, H_l)$	1.981916	1.989040	1.986747	1.987881	1.991376	1.992376	1.991991	1.989567	1.989510	1.989022

Table 11: Summary of IID restart tests for IDQ20MC1

The lowest value for IDQ20MC1 of H is 1.981916 which occurs at -30°C.

The results show that the restart data produced by the chip is always in the required range and that the entropy quality produced by the chip is not affected by the change in working environment.

Snip of restart data tests for IDQ250C3 at -10°C:

```
Opening file: 'IDQ250C3_at-10_restart.bin'
Loaded 1000000 samples made up of 4 distinct 2-bit-wide symbols.
H_I: 1.969534
ALPHA: 5.0251553006530614e-06, X_cutoff: 320
X_max: 312

Restart Sanity Check Passed...

Running IID tests...

Running Most Common Value Estimate...
Literal MCV Estimate: mode = 255592, p-hat = 0.25559199999999999, p_u =
0.25671556044326982
      Most Common Value Estimate (Rows) = 1.961757 / 2 bit(s)
Literal MCV Estimate: mode = 255592, p-hat = 0.25559199999999999, p_u =
0.25671556044326982
      Most Common Value Estimate (Cols) = 1.961757 / 2 bit(s)

H_r: 1.961757
H_c: 1.961757
H_I: 1.969534

Validation Test Passed...

min(H_r, H_c, H_I): 1.961757
```

Test Results for non-IID assessment

The devices pass also the non-IID test and here are the worst-case result to show that the 1.75 entropy per 2-bit sample is still valid even with pessimistic estimators.

Non-IID test:

Model	min(H_o, 2xH_b)	Temperature
IDQ250C2	1.810845	15°C
IDQ250C3	1.760780	-20°C
IDQ6MC1	1.807423	30°C
IDQ20MC1	1.827089	0°C

Restart test:

Model	min(H_r, H_c, H_I)	Temperature
IDQ250C2	1.810845	15°C
IDQ250C3	1.760755	75°C
IDQ6MC1	1.807423	30°C
IDQ20MC1	1.827089	0°C

Snip of non-IID tests for IDQ250C3 at -20°C:

```
Opening file: 'IDQ250C3_at-20_iid.bin'
Loaded 10485760 samples of 4 distinct 2-bit-wide symbols

Number of Binary Symbols: 20971520


Running non-IID tests...


Running Most Common Value Estimate...

Bitstring MCV Estimate: mode = 10574076, p-hat = 0.50421123504638676, p_u =
0.50449246186586993

        Most Common Value Estimate (bit string) = 0.987095 / 1 bit(s)
```

```
Literal MCV Estimate: mode = 2662103, p-hat = 0.25387792587280272, p_u =
0.25422413184778053

        Most Common Value Estimate = 1.975827 / 2 bit(s)


Running Entropic Statistic Estimates (bit strings only)...

Bitstring Collision Estimate: X-bar = 2.5035355550910428, sigma-hat =
0.49998752953766851, p = 0.5

        Collision Test Estimate (bit string) = 1.000000 / 1 bit(s)

Bitstring Markov Estimate: P_0 = 0.49578876495361329, P_1 = 0.50421123504638676,
P_0,0 = 0.49212753558735545, P_0,1 = 0.50787246441264455, P_1,0 =
0.49938878820239235, P_1,1 = 0.50061121179760759, p_max = 7.3322793752741447e-39

        Markov Test Estimate (bit string) = 0.989695 / 1 bit(s)

Bitstring Compression Estimate: X-bar = 5.2153351400449433, sigma-hat =
1.0168831651226147, p = 0.025695490105172469

        Compression Test Estimate (bit string) = 0.880390 / 1 bit(s)


Running Tuple Estimates...

Bitstring t-Tuple Estimate: t = 20, p-hat_max = 0.52010515471632324, p_u =
0.52038616405766824

Bitstring LRS Estimate: u = 21, v = 47, p-hat = 0.50884338456341605, p_u =
0.50912457736632322

        T-Tuple Test Estimate (bit string) = 0.942345 / 1 bit(s)

Literal t-Tuple Estimate: t = 9, p-hat_max = 0.26728171737745793, p_u =
0.26763373976508881

Literal LRS Estimate: u = 10, v = 23, p-hat = 0.26506097742279194, p_u =
0.26541206518767441

        T-Tuple Test Estimate = 1.901668 / 2 bit(s)

        LRS Test Estimate (bit string) = 0.973909 / 1 bit(s)

        LRS Test Estimate = 1.913694 / 2 bit(s)


Running Predictor Estimates...
```

```
Bitstring MultiMCW Prediction Estimate: N = 20971457, Pglobal' =
0.50195582124457627 (C = 10520847) Plocal can't affect result (r = 24)

        Multi Most Common in Window (MultiMCW) Prediction Test Estimate (bit
string) = 0.994368 / 1 bit(s)

Literal MultiMCW Prediction Estimate: N = 10485697, Pglobal' = 0.25254680524917189
(C = 2644507) Plocal can't affect result (r = 12)

        Multi Most Common in Window (MultiMCW) Prediction Test Estimate = 1.985377
/ 2 bit(s)

Bitstring Lag Prediction Estimate: N = 20971519, Pglobal' = 0.50039298358788309 (C
= 10488103) Plocal can't affect result (r = 23)

        Lag Prediction Test Estimate (bit string) = 0.998867 / 1 bit(s)

Literal Lag Prediction Estimate: N = 10485759, Pglobal' = 0.25041593021132424 (C =
2622189) Plocal can't affect result (r = 13)

        Lag Prediction Test Estimate = 1.997602 / 2 bit(s)

Bitstring MultiMMC Prediction Estimate: N = 20971518, Pglobal' =
0.50446409060123487 (C = 10573480) Plocal can't affect result (r = 24)

        Multi Markov Model with Counting (MultiMMC) Prediction Test Estimate (bit
string) = 0.987177 / 1 bit(s)

Literal MultiMMC Prediction Estimate: N = 10485758, Pglobal' = 0.2538558962147302
(C = 2658243) Plocal can't affect result (r = 12)

        Multi Markov Model with Counting (MultiMMC) Prediction Test Estimate =
1.977918 / 2 bit(s)

Bitstring LZ78Y Prediction Estimate: N = 20971503, Pglobal' = 0.50448438303543686
(C = 10573898) Plocal can't affect result (r = 24)

        LZ78Y Prediction Test Estimate (bit string) = 0.987118 / 1 bit(s)

Literal LZ78Y Prediction Estimate: N = 10485743, Pglobal' = 0.2540579571716256 (C =
2660357) Plocal can't affect result (r = 12)

        LZ78Y Prediction Test Estimate = 1.976770 / 2 bit(s)


H_original: 1.901668

H_bitstring: 0.880390

min(H_original, 2 X H_bitstring): 1.760780
```

Snip of restart tests for IDQ250C3 at 75°C:

```
Opening file: 'IDQ250C3_at75_restart.bin'
Loaded 1000000 samples made up of 4 distinct 2-bit-wide symbols.

H_I: 1.837853

ALPHA: 5.0251553006530614e-06, X_cutoff: 347

X_max: 305


Restart Sanity Check Passed...


Running non-IID tests...


Running Most Common Value Estimate...

Literal MCV Estimate: mode = 253380, p-hat = 0.25337999999999999, p_u =
0.25450034884898232

        Most Common Value Estimate (Rows) = 1.974260 / 2 bit(s)

Literal MCV Estimate: mode = 253380, p-hat = 0.25337999999999999, p_u =
0.25450034884898232

        Most Common Value Estimate (Cols) = 1.974260 / 2 bit(s)


Running Tuple Estimates...

Literal t-Tuple Estimate: t = 7, p-hat_max = 0.26509322787647183, p_u =
0.26623015528943267

Literal LRS Estimate: u = 8, v = 19, p-hat = 0.26058712253093869, p_u =
0.26171779619562802

Literal t-Tuple Estimate: t = 8, p-hat_max = 0.27927084270511099, p_u =
0.28042646560814599

Literal LRS Estimate: u = 9, v = 22, p-hat = 0.29392023420665114, p_u =
0.29509366889459004

        T-Tuple Test Estimate (Rows) = 1.909254 / 2 bit(s)
```

```
        T-Tuple Test Estimate (Cols) = 1.834306 / 2 bit(s)

        LRS Test Estimate (Rows) = 1.933916 / 2 bit(s)

        LRS Test Estimate (Cols) = 1.760755 / 2 bit(s)


Running Predictor Estimates...

Literal MultiMCW Prediction Estimate: N = 999937, Pglobal' = 0.25221585111160211 (C
= 251083) Plocal can't affect result (r = 10)

        Multi Most Common in Window (MultiMCW) Prediction Test Estimate (Rows) =
1.987269 / 2 bit(s)

Literal MultiMCW Prediction Estimate: N = 999937, Pglobal' = 0.25157185822612754 (C
= 250440) Plocal can't affect result (r = 10)

        Multi Most Common in Window (MultiMCW) Prediction Test Estimate (Cols) =
1.990958 / 2 bit(s)

Literal Lag Prediction Estimate: N = 999999, Pglobal' = 0.25126784440196814 (C =
250152) Plocal can't affect result (r = 12)

        Lag Prediction Test Estimate (Rows) = 1.992702 / 2 bit(s)

Literal Lag Prediction Estimate: N = 999999, Pglobal' = 0.25108357066867415 (C =
249968) Plocal can't affect result (r = 11)

        Lag Prediction Test Estimate (Cols) = 1.993760 / 2 bit(s)

Literal MultiMMC Prediction Estimate: N = 999998, Pglobal' = 0.25387594332841612 (C
= 252756) Plocal can't affect result (r = 9)

        Multi Markov Model with Counting (MultiMMC) Prediction Test Estimate (Rows)
= 1.977804 / 2 bit(s)

Literal MultiMMC Prediction Estimate: N = 999998, Pglobal' = 0.25362657769828872 (C
= 252507) Plocal can't affect result (r = 10)

        Multi Markov Model with Counting (MultiMMC) Prediction Test Estimate (Cols)
= 1.979222 / 2 bit(s)

Literal LZ78Y Prediction Estimate: N = 999983, Pglobal' = 0.25412110572791186 (C =
252997) Plocal can't affect result (r = 10)

        LZ78Y Prediction Test Estimate (Rows) = 1.976412 / 2 bit(s)

Literal LZ78Y Prediction Estimate: N = 999983, Pglobal' = 0.25400393245216935 (C =
252880) Plocal can't affect result (r = 10)
```

```
        LZ78Y Prediction Test Estimate (Cols) = 1.977077 / 2 bit(s)


H_r: 1.909254

H_c: 1.760755

H_I: 1.837853


Validation Test Passed...


min(H_r, H_c, H_I): 1.760755
```