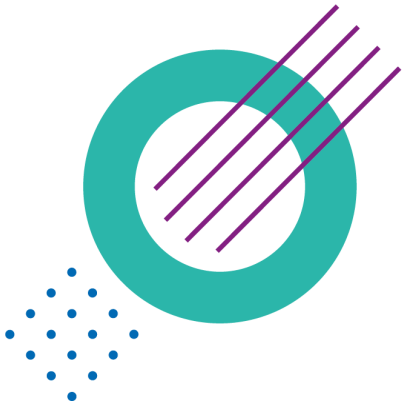


Quintessence Labs

Data Uncompromised

QuintessenceLabs

SP 800-90B Non-Proprietary
Public Use Document

qStream 100 version 1.5 Entropy Source

Hardware: QRNG version 3.1
Software: qStream 100 version 1.5

Document Version: 1.1
Document Status: Released
Document Date: 21 October, 2024

Prepared by:

TERON LABS

Unit 3, 10 Geils Court
Deakin ACT 2600
Australia

+61 2 5114 4878
info@teronlabs.com
www.teronlabs.com

Vendor:

QuintessenceLabs

Unit 11, 18 Brindabella Circuit
Brindabella Business Park
Canberra Airport, ACT 2609
Australia

Contents

Document Management

Version	Date	Author	Description
d2	22 February, 2024	Yvonne Cliff	Initial Draft
d2_q2	23 February, 2024	A.Labios	Added qLabs logo
1.0	26 February, 2024	Yvonne Cliff	Initial Release
1.1	18 October, 2024	Yvone Cliff, Uyen Dinh	Add OE5 and OE6; fix typographical error in OE4 name

1. Description

This document is the Public Use Document for the NIST SP 800-90B Entropy Source Validation of the QuintessenceLabs qStream 100 version 1.5 entropy source.

This entropy source is a physical (P) source and provides a Quantum Random Number Generator (QRNG) that consists of a PCIe (Gen2) card containing the noise source and software components that control the noise source, monitor the QRNG outputs, and allow raw data and output from the Random Bit Generator (RBG) construction to be drawn.

Random bits are created by measuring the quantum tunnelling noise of a tunnel diode, which is a random physical process. The raw analog noise measurements are amplified and digitised. This results in 12-bit representations of the measurements which are then reduced to 8-bit samples. To condition the samples, the QRNG uses CMAC AES-128 (as specified in NIST SP 800-38B), which is a vetted conditioning component. The output of the conditioning function is a full entropy bitstream. A small part of this bitstream is used for seeding a CTR_DRBG using AES-128 (without a derivation function). This DRBG and the rest of the full entropy bitstream from the CMAC conditioner are used to implement the RBG construction XOR-NRBG from the second draft of SP 800-90C to provide an RBG construction outputting a full entropy bitstream to the end user.

The qStream 100 version 1.5 is designed to be operated in a Linux operating system (e.g. RedHat, Debian or Ubuntu).

Implementation of health testing is split across the PCIe card and the software.

Errors encountered during operation will be flagged via the error output channel. Detected errors will block the XOR-NRBG output but not that of the raw data. Raw data which passes through the raw data output interface is never used in the CMAC conditioner or XOR-NRBG construction.

Names and versions for the hardware, software and entropy source are listed in Table 1. Tested operational environments are listed in Table 2.

The standard versions applicable to this submission are listed in Table 3. The XOR-NRBG construction is compliant with the second draft of SP 800-90C. It is not compliant to the third draft due to the security strength of the DRBG in use.

Table 1 – Software, Hardware and Entropy Source Versions

Type	Name	Description	Version
Hardware	QRNG	PCIe (Gen 2) card, with Xilinx Artix-7 (xc7a200t) FPGA, bias circuit, and tunnel diode	3.1
Software	qStream 100	The software controls the noise source, monitors QRNG outputs, allows raw and XOR-NRBG output to be drawn, and implements part of the health testing	1.5
Entropy Source	qStream 100	The entropy source consists of the hardware and software components listed above	1.5

Table 2 – Tested Operational Environments

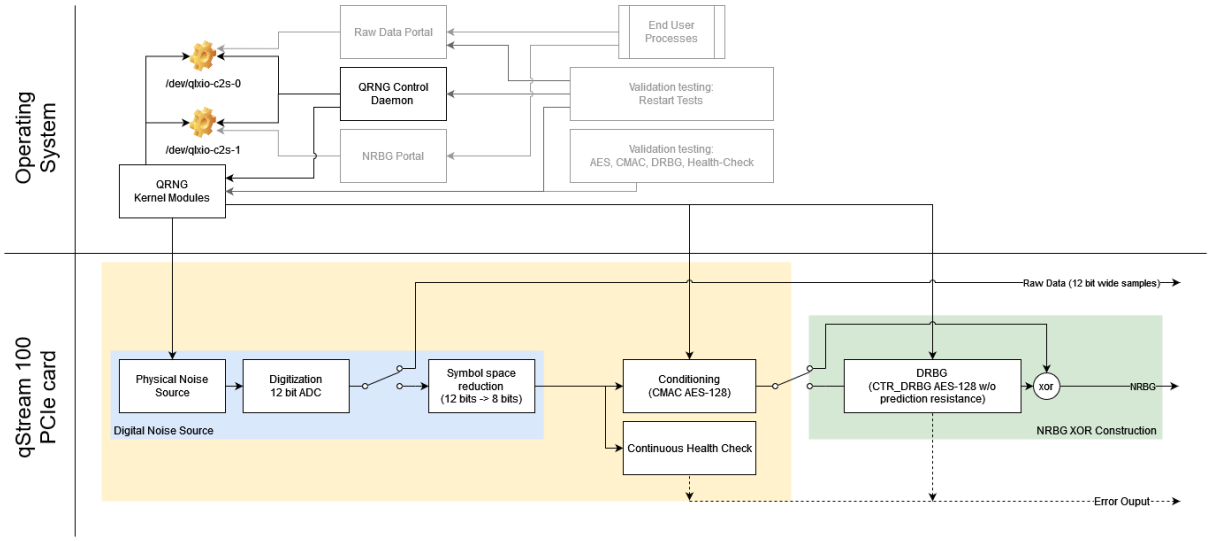
Reference	Platform	CPU/Processor of the platform	Operating System
OE1	Dell Optiplex 7000	12th Gen Intel Core i7-12700 2.1 GHz	Ubuntu Server 22.04
OE2	Dell R350 server	Intel Xeon E-2314 2.8 GHz	Debian 12
OE3	Dell R6615 server	AMD EPYC 9224 2.50 GHz	Red Hat 8.8
OE4	Dell R640 server	Intel Xeon Silver 4214R 2.40 GHz	Red Hat 8.6
OE5	Dell PowerEdge R350	Intel Xeon E-2378 2.60 GHz	Debian 12
OE6	Dell R360 server	Intel Xeon E-2434 at 3.4 GHz	Red Hat 8.8
Note: All OEs include the hardware PCIe card, QRNG version 3.1			

Table 3 – Applicable Standards

Document	Title	Date
SP 800-90B	*Recommendation for Entropy Sources Used for Random Bit Generation*	Jan 2018
SP 800-90A	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*	June 2015
SP 800-90C	*Recommendation for Random Bit Generator (RBG) Constructions (2nd Public Draft)*	Apr 2016
Implementation Guidance	*Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program*	Jan 2024

2. Security Boundary

Figure 1 shows the security boundary.



Components in gray boxes are not part of the Security Boundary.

Figure 1 – qStream 100 v1.5 component overview.

The entropy source includes the following components:

- Components on the PCIe card:
  - Physical noise source (tunnel diode).
  - Digitization with a 12-bit ADC (Analog to Digital Converter) and symbol space reduction to 8 bits (equivalent to an 8-bit ADC).
  - Conditioning component CMAC with AES-128
  - Hardware component of the health tests implementation.
- Components in software:
  - The QRNG control daemon and QRNG kernel modules *qlxio* and *xdma_k7.*
    - These monitor and control the noise source and provide the software component of the health tests implementation.
  - Operating system device nodes */dev/qlxio-c2s-0* and */dev/qlxio-c2s-1*
  - 128 MB buffer of XOR-NRBG output required for correct health test operation.

The security boundary includes the entire PCIe card as well as the software components of the entropy source listed above. The CTR_DRBG and the XOR-NRBG construction are included in the security boundary but not the entropy source. The security boundary also includes a 128 MB software buffer which buffers the output of the XOR-NRBG; this buffer is required for correct operation of the continuous health tests and is therefore part of the entropy source as well.

3. Operating Conditions

The qStream 100 version 1.5 random number generator is designed to be operated in a personal computer or server environment. It is powered from the standard 12V + 3.3V voltage lanes provided by the PCI Express bus; an additional power supply is not required.

While the operating temperature range of the diode provided in the datasheet lies between -55 and 100°C, the card itself is specified to operate at temperatures between -15 and 60°C, due to more restrictive requirements of other components. Entropy tests have been performed at

temperatures ranging from 54°C to 83°C. Normally a fan or cooling system is available in the card's normal operating environment (e.g. inside a server).

The entropy source adjusts the voltage supplied to the tunnel diode from 0 mV up to the optimal voltage each time the entropy source is restarted. This peak operating point voltage typically lies around 65 mV but varies from card to card. During operation of the entropy source, the QRNG control daemon tracks and adjusts the operating point to maximize the quantum signal-to-noise ratio (QSNR) and gain maximum shot noise. The voltage supplied to the tunnel diode will not exceed 350 mV.

4. Configuration Settings

Various configuration settings are stored in the file /usr/local/etc/hrng.ini. Settings that must not be changed from the values provided by QuintessenceLabs are listed below. If any changes are made, this would invalidate the SP 800-90B entropy certification.

The following settings concern the health tests required for SP 800-90B compliance and must not be changed from the values listed:

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
[healthcheck-v21]
repetition_threshold = 6
adaptative_threshold = 27
repetition_l2_enabled = 1
repetition_l2_threshold = 4
repetition_l2_window = 52

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
[autocutoff]
enabled = 0
```

The following setting determines the type of conditioning to use and must not be changed from *nrbg*.

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
[conditioning]
; The type of conditioning to use. One of:
; nrbg, drbg, cmac, nacf, zero
;
; Note: Do NOT change this unless you know what you are doing.
type = nrbg
```

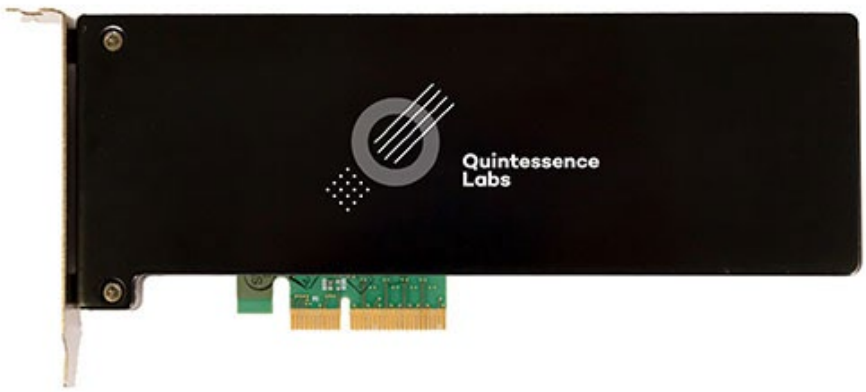
The following parameters determine how the entropy source adjusts the tunnel diode voltage. This affects how much entropy the tunnel diode provides. These parameters will be adjusted by QuintessenceLabs to the optimal values for each card and should not be changed from the values provided with the entropy source. The values provided by QuintessenceLabs with the entropy source may be different to the ones below. Inappropriate adjustment of these values will be detected by the entropy source health tests.

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
[monitoring-v21]
; although this section is for v2.1, these settings also apply to v3 cards
; Entropy target settings.
entropy_target = 4.8
entropy_operating_range = .08
```

5. Physical Security Mechanisms

The entropy source is encapsulated in an opaque metal housing that shields it from electromagnetic interference and direct access. It is assumed that the card is operated in an environment with restricted physical access (e.g. server room). An image of the card is provided in Figure 2.

Figure 2 – QRNG card



6. Conceptual Interfaces

The entropy source provides the following interfaces:

- qstream_nrbg_get_bytes(): Obtains conditioned entropy for the caller. This interface corresponds to the GetEntropy() conceptual interface from SP 800-90B and provides a full entropy bitstream for operational use.
- qstream_noise_get_bytes(): Obtains raw noise data for testing purposes. This interface corresponds to the GetNoise() conceptual interface from SP 800-90B and can be used to gather noise source samples for optional independent testing.

These interfaces are made available to the Linux OS via the two device nodes /dev/qlxio-c2s-0 and /dev/qlxio-c2s-1, respectively.

An interface to reset the card (which is the mechanism for requesting on-demand health tests) is also provided.

In addition, status information and throughput information may also be requested.

Further information on the use of the above conceptual interfaces is available in the **qStream100-1.5-UserGuide**.docx/pdf provided with the product.

7. Min-Entropy Rate

The entropy source outputs a full entropy bitstream according to the FIPS 140-3 IG D.K Resolution 19 definition.

8. Health Tests

Description of Individual Tests

The following health tests are implemented to meet the SP 800-90B health testing requirements, and operate on data that is passed to the conditioner (but not on data sent to the raw data interface):

- A modified Repetition Count Test (RCT) with two cutoffs, $C_1 = 6$ and $C_2 = 4$.
  - The first level of the test records when C_1 or more identical consecutive samples occur in a window of size $w_1 = 10\ \text{million}$ samples, for the last $w_2 = 52$ windows.
  - The second level of the test triggers a **health test failure** when there are C_2 or more recorded first level RCT flags in the last $w_2 = 52$ windows of size w_1 samples.
  - Data is buffered in a 128 MB software buffer to ensure the health test has passed before the data is provided to the user.
- An Adaptive Proportion Test (APT) as specified in the SP 800-90B standard with cutoff $C = 27$ and window size of 512 samples. Any failure of the APT triggers a **health test failure**.

The following health tests are also implemented, but are not required to meet the SP 800-90B requirements:

- Periodic testing (by default every 5 seconds), which requests data from the raw data interface and performs entropy estimations and an assessment of the distribution of the data. Any failure of the data to meet the expected minimum entropy level and closeness of the distribution to the expected one will cause a **health test failure**.
- BIST/known-answer tests performed on all CMAC, DRBG, and AES-ECB functions.

Health Test Failures

Health test failures are handled in the following way:

- The control daemon continuously monitors the error registers of the cryptographic functions (e.g. CMAC, DRGB, AES) and of the health tests.
- If any error has been raised by any of the subcomponents, output from the XOR-NRBG conditioned data interface is blocked and the card is restarted. This triggers a re-training of the card that includes:
  - Determining the optimal operating point (bias voltage) of the tunnel diode
  - Executing the startup health tests
  - Flushing all buffers containing outputs from the entropy source

    - In the case where the startup health tests and the continuous health tests are OK, the control daemon assumes that an intermittent failure has triggered the error.
- The failure of any test as well as any automatically triggered restart is logged.
- In the case where the automatically triggered restart did not provide clean test results, the XOR-NRBG output is stopped and it is assumed that a persistent failure has occurred. This error is also logged.

Types of Health Tests

The following types of health tests are implemented:

- Startup health tests consist of the modified RCT, the APT and the periodic testing described above, and are performed every time the card is restarted before any data is made available to end users. The modified RCT and APT are run for three seconds, during which time they will process approximately 1.5 billion samples. After these tests have passed, all buffers are flushed and fresh data is generated before the user may request any data from the output interfaces. The BIST/known-answer tests are also performed at startup.
- Continuous health tests consist of the modified RCT and the APT.
- Periodic testing is performed, by default every five seconds. The periodic testing is not classified as a continuous health test and is not part of the requirements of SP 800-90B.
- On-demand testing is performed by requesting a card reset, which will execute the startup tests.

Known Failure Modes

Known failure modes will be detected by the continuous health tests. Known failure modes are:

- Failure of the tunnel diode (shorted diode and failed-open diode). These failure modes are very rare and will result in zero entropy from the tunnel diode. This will be detected by the continuous health tests.
- Bias voltage of the tunnel diode being too low or too high, resulting in reduced or zero entropy being generated by the tunnel diode. This will be detected by the continuous health tests before the output entropy rate from the conditioner drops below full entropy.

9. Maintenance

Instructions for installing the entropy source software before the first use of the entropy source are provided in the **qStream100-1.5-UserGuide**.docx/pdf provided with the product.

The qStream 100 is designed to be operated in a high-availability server environment. The control daemon continuously runs in the background to monitor the error registers of the system's cryptographic algorithms (e.g. CMAC, DRGB, AES) and of the continuous health checks, and automatically performs necessary tasks to ensure that the entropy source is available and produces high-quality output.

If the operating conditions are met as stated above, no additional maintenance is required to be performed by the user.

10. Required Testing

Startup and continuous health testing provided by the entropy source will stop output from the entropy source before the output entropy rate from the conditioner drops below full entropy. Therefore, there is no requirement for the user to perform further testing.

The following tests may be performed by the user and are optional:

- Validation testing on the cryptographic functions (AES, CMAC, and DRBG) and the continuous health tests can be performed during normal operation by temporarily putting the QRNG into test mode. This pauses the random number generation for end-users. Test vectors can then be injected, tests run, and the results read back. After the tests have been executed, the entropy source will go back to its operational mode with all pre-test-mode parameters being used. The detailed procedure is outlined in application note ARAS 0006689, titled *qStream – Independent Validation Testing*, version 3.1.
- Testing of raw data (described below).
- Testing of conditioned data (described below).

Raw Noise Testing

To confirm that the entropy source is working properly, raw noise data can be obtained from the card and tested manually. The software includes a number of scripts that can be used for this purpose. For example, to generate a noise data set of 1,000,000 bytes (1 byte = one 8-bit sample) and execute the entropy estimation tests on the obtained data set, execute the following commands:

```
python qstream-noise.py --bytes 1000000 -f noise
./ea_non_iid noise 8
```

The output of the entropy estimation will be similar to the following:

```
Running non-IID tests...
Running Most Common Value Estimate...
Running Entropic Statistic Estimates (bit strings only)...
Running Tuple Estimates...
Running Predictor Estimates...
H_original: 6.565841
H_bitstring: 0.655881
min(H_original, 8 X H_bitstring): 5.247049
```

The result of the entropy estimation will vary, but `min(H_original, 8 X H_bitstring)` is normally 4.5 or greater.

Conditioned Data Testing

To obtain a sample of conditioned data and run it through the Dieharder test suite, the following set of commands can be used.

```
python qstream-nrbg.py --bytes 4G --file nrbg.bin
./dieharder -a -g 201 -D default -D histogram -f nrbg.bin
```