SwiftRNG

SwiftRNG Z – April 2019 – Rev 1.0

SwiftRNG Z is a Hardware Random Number Generator that can produce high quality true random numbers at a rate of 80 Mbit/s. Manufactured as a USB device, it is compatible with most server oriented operating systems and hardware platforms. It is designed to comply with NIST SP 800-90B (second draft): "*Recommendation for the Entropy Sources Used for Random Bit Generation".*

Core capabilities

- Generation performance – 80 Mbit/s generation speed through a USB 2.0 High Speed interface
- Backward compatible with SwiftRNG, SwiftRNG Pro and SwiftRNG LE
- Device cluster scalability and fail-over capabilities through provided software API on Linux, Windows and macOS platforms
- Windows 7/8.1/10 compatibility through provided Entropy Server application and software API
- Device API - enables independent security testing and validation of the entropy source in compliance with NIST SP 800-90B (second draft)
- Build-in Linear Corrector (P. Lacharme) using a 0.5 compression rate.
- Optional additional post processing methods available - SHA-256, SHA-512, XorShift64
- Real-time validation of each noise source and entropy output – provides confidence of device operation correctness
- On demand built-in diagnostics that can be triggered through device API and software API

Description

The core functionality of the SwiftRNG Z device relies on two identical electrical circuits that utilize Zener breakdown effect (due to quantum tunneling) and serve as independent noise sources. The Zener Breakdown is observed in Zener diodes that have Vz less than 5V and a negative thermal coefficient (TC). Zener diodes used in this device have a negative TC and operate at about 4.6 breakdown voltage. The electrical noise produced by noise sources are digitized into random byte streams and inspected using build-in health diagnostics. The random bytes produced by both noise sources are combined and processed internally with a Linear Corrector, a technique proposed by P. Lacharme ("Post-Processing Functions for a Biased Physical Random Number Generator". In: FSE 2008. LNCS, vol. 5086, pp. 334-342. Springer-Verlag. 2008), using a 0.5 compression rate. A monitoring logic checks the quality of the final random bytes produced by continuously running 'Repetition Count Test' and 'Adaptive Proportion Test' tests.

It is possible to use two or more SwiftRNG Z devices to additively increase the random number generation speed. The software API seamlessly integrates multiple devices and uses them concurrently as a single stream of random data. The API will monitor the health of the cluster and will resize the cluster on-the-fly, allowing device swapping in real-time. This makes it possible to remove and add SwiftRNG Z devices in the middle of random number generation.

Supported systems

- Linux (x86, x64) – data access provided through loadable device driver, program utilities or software API on Ubuntu, Red Hat, CentOS 7, CentOS 6.6 and other Linux based x86-64 systems.
- macOS 10.6 and up – data access provided through software API or program utilities
- Windows 7, 8.1, and 10 – data access provided through software API, DLL, Entropy Server application or program utilities

Applications

The SwiftRNG Z is a versatile device that can be used for a wide range of purposes, including, but not limited to:

- Cryptography
- Authentication
- Payment services
- Secure key generation
- Research (statistical sampling)
- Computer simulations
- Gaming and lotteries

Product Specifications

Product name	SwiftRNG Z
Interface	USB 2.0 high-speed interface with EMI filtering (also compatible with full-speed 1.1 interface)
Entropy final output	Download speed: 80 Mbit/s Entropy score: full entropy
Noise source	Two independent circuits based on Zener breakdown effect (due to quantum tunneling) in reversed-biased Zener diodes
Health tests	Start-up and continuous health diagnostics of random noise sources. Continuous 'Repetition Count' and 'Adaptive Proportion' statistical tests of the entropy source.
NIST compliance	NIST SP 800-90B (second draft), NIST SP 800-22
Validation tests	Diehard, Dieharder, NIST, Rngtest, Ent, Crush and BigCrush
Supported systems	Linux, macOS and Windows 7/8.1/10
Data interface software	Software API and utilities with a complete source code available for Windows, macOS and Linux. A loadable module driver for Linux with a complete source code.
Power consumption	Draws no more than 180 mA
Enclosure material	ABS
Weight	Less than 22 grams (0.77 Oz)
Dimensions	78mm * 23mm * 14mm
RoHS compliance	All parts and materials are RoHS compliant
Average EMF emission	Less than 1 μW/m² measured at the surface of the device

Patents

US Patent 9,477,443 issued – "*Method and apparatus of entropy source with multiple hardware random noise sources and continuous self-diagnostic logic*".

Operating Temperatures

- Maximum device operating temperature: 149°F (65°C). The temperature is measured on the bottom surface of the device in the middle area.
- Ambient temperature: Min: 32°F (0° C), max: 81°F (27° C). The connected device should be located at least 1 inch away from other USB devices in an area with a free or forced air flow circulation.

User Notes

- The SwiftRNG device can be plugged into one of the available USB 2.0 or 3.0 ports directly or by use of an USB 2.0 ‘A’ male to ‘A‘ female extension cable (extension cable not included).
- Do not immerse this product in any liquid or expose it to direct sunlight or high temperature environment
- The software installation and configuration instructions can be found online at the following web address: https://tectrolabs.com/docs/swiftrng/

Device API Specifications

The SwiftRNG Z device API is implemented using a USB High Speed interface utilizing bulk data transfers. It operates based on 1-byte commands. We recommend using the supplied software kit, as it reduces the complexity and simplifies the use of the generator. The following table contains the complete command set and descriptions.

Command	Response	Description
'x'	16,000 random bytes + the status byte	The response will contain 16,000 low biased (RAW) random bytes and an additional byte for the status byte. The status byte will contain 0 value for success or error code.
'm'	8 bytes of the device model + the status byte	The response will contain 8 bytes for the device model as ASCII codes. The status byte will contain 0 value for success or error code.
'v'	4 bytes of the device version + the status byte	The response will contain 4 bytes for the device version as ASCII codes. The status byte will contain 0 value for success or error code.
's'	15 bytes of the device serial number + status byte	The response will contain 15 bytes for the device serial number as ASCII codes. The status byte will contain 0 value for success or error code.
'f'	512 bytes that represent frequency tables of the noise sources + the status byte	The first 256 bytes are frequency table of the first noise source and the next 256 bytes are frequency table of the second noise source. The status byte will contain 0 value for success or error code.
'<'	16,000 random bytes + the status byte	The response will contain 16,000 of RAW unprocessed and unmodified random bytes generated from the first noise source. The status byte will contain 0 value for success or error code.
'>'	16,000 random bytes + the status byte	The response will contain 16,000 of RAW unprocessed and unmodified random bytes generated from the second noise source. The status byte will contain 0 value for success or error code.
'd'	Status byte	The command will trigger the built-in device diagnostics. The status byte will contain 0 value for success or error code.

One-Year Limited Warranty: TectroLabs offers a 1-year limited warranty on the SwiftRNG Z. We will replace (at our sole discretion) any device that fails due to defect in materials or manufacturing.