User Manual

Infinite Noise TRNG

Document Version: 1.1

open-source true random number generator

According to the european WEEE directive, electrical and electronic and electronic must not be disposed with consumers waste. Its components must be recycled or disposed apart from each other. Otherwise contaminative and hazardous substances can pollute our environment.

You as a consumer are commited by the law to dispose electrical and electronic devices to the producer, the dealer, or public collecting points at the end of the devices lifetime for free. Particulars are regulated in national right. The symbol on the product, in the user's manual, or at the packaging alludes to these terms. With this kind of waste separation, application and waste disposal of used devices you achieve and important share to environmental protection.

13-37.org electronics – owner: Manuel Domke
Adelheidstr. 59 - 65185 Wiesbaden – Germany
WEEE-Reg: DE86896758 VAT No: DE313047369

Table of contents

1. Introduction

Thank you for supporting the Infinite Noise TRNG on Crowd Supply!

Modular entropy multiplication was invented by Peter Allen in 1999 and later reinvented by Bill Cox and Peter Allen simultaneously (in different styles).

The Infinite Noise hardware design was created by Bill Cox (and more contributors) in 2014 and is available under a public domain license.

The hardware design was not modified by me – I just found the GitHub project and wanted to have one.

So I started making them by myself and am now supporting the project with further development and by making it available to you!

Help me by reporting bugs and/or requesting features!

2. Safety instructions

Please read this manual carefully before using the product for the first time. Otherwise damage may result!

- Don't place the device in direct sunlight or places with high temperatures.
- Don't expose the device to water, moisture or high humidity.
- Don't try to open or modify the device.
- Always keep packing materials away from children.

2.1. Operating Environment

This device is designed to be used in private households.

2.2. Cleaning

- Disconnect the device from your computer before cleaning.
- Use a soft, slightly humid cloth to clean the outer case of the device.
- Do not use alcohol or solvent based cleaners. These may damage the surface of the polycarbonate case.

3. First Use

3.1 Verification and Registration

To assert that your device arrived in the condition it was made by 13-37.org electronics and has not been modified/tampered on its way,
you can verify and register its serial number online:

13-37.org/verify

Registration is optional - but you can even do it anonymously.

The main purpose of this is to enable you to verify that the device wasn't modified on its way to you, so published unregistered serials pose a risk to the process.

Even if you don't care about your device's integrity (like you don't want it to use for cryptography), please register it to support this process, as its essential that the serial numbers stay unique.

The serial is stored on the USB chip and also printed on the security labels at the edges, so anyone who has seen your device could use it to build fake or even tampered devices that look valid on that online service (until someone else registers it).

If that should ever happen and I get note of it, I'll have to invalidate those serials. This has no effect on the device operation, but it'll show up as invalid on the website.

The verification described on the next page is a better way to verify its correct operation, but you need the driver installed for it.

3.2 Driver installation

Before using the Infinite Noise TRNG for the first time, you'll need to download and install the driver from:

13-37.org/AM7cQ or **git.io/vp2DD**

You can also compile it from source if you prefer, but all packages are signed with the following PGP Key and there is a reference to the corresponding Github commit in the version output.

Releases are built from a fork of the original Infinite Noise Project from Bill Cox (waywardgeek):

https://github.com/13-37-org/infnoise | https://github.com/waywardgeek/infnoise

PGP Key Fingerprint:
You can also find the fingerprint on my website (13-37.org/keys/), the Crowd Supply campaign and on Github!

```
71AE 099B 262D C0B4 93E6 EE71 975D C25C 4E73 0A3C
```

Version Output:

```
$ infnoise -version
GIT VERSION - 0.2.4-14-g61d534e
GIT COMMIT  - 61d534ef1de6992d1fe89aadeca7367ba93e2578
GIT DATE    - 2018-04-16T18:39:15+02:00
```

3.3 Verification of operation

With the driver installed you can now actually verify that the device works as expected.

Run it in debug mode and check that the highlighted values are in the range of +/- 3% of the given example:

```
$ infnoise --debug -no-output
Generated 1048576 bits.  OK to use data.
Estimated entropy per bit: 0.874112, estimated K: 1.832880
num1s:50.538887%, even misfires:0.100875%,
odd misfires:0.191457%
```

The health monitor also does this in normal operation and does not output data that does not match the expected entropy. (then it would output "NOT OK" instead of "OK"..)

As long as data is coming from the driver - and you've verified the driver's integrity - everything is fine.

An easy way to verify the driver's integrity is to use the provided packages after you've checked the signatures. Check the FAQ on 13-37.org on how to do it.

When you compile the driver from source, I recommend using a commit that also was used for a release.

If you do so - and especially if you build it from a tagged commit of the 13-37-org fork - please compare with the released binary and share your results, so we can build trustworthy releases collectively.

Just keep in mind that builds prior to version 0.2.6 were not reproducible as the build date was included in the version output.

4. Features

4.1. Unix service

The linux packages will install a service that starts the driver when the device is plugged in.

In default configuration random data is written to /dev/random.

You can check the service state like this:

```
$ sudo service infnoise status
```

4.1.1. Configuration file

You can configure additional environment variables for the service in the configuration file at /etc/infnoise.conf.

All parameters are optional.

INFNOISE_MULTIPLIER	output multiplier
INFNOISE_SERIAL	Specify a serial number to select a specific device
INFNOISE_DEBUG	debug logging to syslog

4.2. Usage of the Command Line Interface (CLI)

For advanced features you may want to use the command line interface in standalone mode.

To do so, it's **necessary** to stop the service:

```
$ sudo service infnoise stop
```

This is not permanent and the service will be restarted when you re-plug the device. To permanently disable use:

```
$ sudo systemctl mask infnoise
```

4.3. Command line parameters

Parameter	Description	Default
--debug	Turn on debug output	Off
--dev-random	Write data to /dev/random, otherwise its written to stdout	off
--raw	Output of raw dara coming from the device, whitening disabled	off
--multiplier	output multiplier; write 256 bits * **value** for each 512 bits written to the Keccak sponge	0 / off
--no-output	No output, only for debugging	off
--pidfile	Filename for PID-File, to be used with --daemon	-
--daemon	Start in background / As daemon	off
--list-devices	List all connected Infinite Noise TRNG's/FT240X	-
--serial	Specify a serial number to select a device	-

4.4. Usage examples

→ *Usage Example 1 (Linux, Debug-Mode, no output of random data)*

```
$ sudo infnoise --no-output --debug
```

→ Usage Example 2 (Linux, output to file „output.rnd")

```
$ sudo infnoise > output.rnd
```

→ Usage Example 3 (feeding /dev/random in daemon mode)

```
$ sudo infnoise --dev-random --daemon
```

→ Usage Example 4 (Windows, output to file „output.txt")

```
C:\infnoise-win.exe output.txt
```

5. Technical Data

Operating voltage:	5V
Current:	8 mA
Interface:	USB 2.0
Temperature Range:	0-60°C
Output rate:	32 kB/s

More technical documentation is available on Github: https://github.com/13-37-org/infnoise

6. Declaration of Conformity

This device corresponds to directives 2014/30/EU and 2011/65/EU.
With the CE sign, 13-37.org electronics, holder Manuel Domke ensures that the product is conformed to the basic standards and directives. A full copy of the declaration of conformity is available online at https://13-37.org/o9FFG