connect tech
stay connected

User Manual
Project Semester 2023

Carlo Bauer
Paul Betsch
Marina Göppel
Stefan Kleinhenz Leiva
Carsten Michel
Lukas Siegle

June 14, 2023

Contents

1 Intended Use

The intended use of this Pendulum is to be a True random bits Generator. A True random bits Generator uses a physical noise source to generate true random bits. The API allows for the regulation of the number of bits the numbers should possess and the quantity in which they should be generated. The random bits can then be used for various applications, such as cryptography, simulation or scientific research.

This prototype of a True random bits Generator(TRNG) was invented and developed in the context of our project semester during the summer of 2023 at the University of Applied Science Mannheim.

1.1 Warnings

i. With this construction there is electricity in most parts. It is recommended to pull all power supplies before you work with or repair the prototype.

ii. All cables are lined with a cable conduit. Please refrain from taking them out and touching them.

iii. While the prototype is active the pendulum swings in a circular motion. Please stay at least 1m away from the pendulum to avoid getting hit.

iv. While the prototype is initialized, do not interfere in any way with the sampling process.

v. Please do not touch any cables or circuit boards integrated in the prototype.

vi. Use the prototype only with a good light setup to ensure no shadows are being captured by the camera. Shadows can massively interfere with the quality of the random bits.

2 Usage

2.1 General REST API Endpoints

This table covers various endpoints and their paths for accessing a random number generator in general. The random number generator produces HEX-encoded bit arrays as its output, with leading zeros added if necessary. To add leading zeros was explicitly wished by the client, we strongly advise against adding leading zeros to an hex-encoded random number in a normal context.

Endpoints	Path	Responses	Definition
GetRandomNums	/randomNum/getRandom	200	successful operation; HEX-encoded bit arrays (with leading zero if required)
		432	system not ready; try init
		500	data generation failed; check noise source
InitRandomNums	/randomNum/init	200	successful operation; random bits generator is ready and random bits can be requested
		409	system already running
		500	functionality not given; check hardware
		555	unable to initialize the random bits generator within a timeout of 60 seconds
ShutdownRandomNums	/randomNum/shutdown	200	successful operation; random bits generator has been set to 'standby mode'
		409	system already shutdown

2.2 How to use the REST API

A REST API allows different software applications to communicate and exchange data over the internet using standardized HTTP protocols. Our REST API provides all the necessary functionalities and logic responsible for the aforementioned requests and the initialization of the TRNG and its associated components.

To use the REST API you can choose a HTTP client of your choice e.g. Postman or Curl. In the following enumaration we explain how to interact with the API using Curl.

1. First of all it's necessary to initialize the TRNG with the following command:

```
curl https://172.16.78.60:5520/trng/randomNum/init
```

2. If the request returns a status code 200 you can start generating random bits. To get random bits use following command:

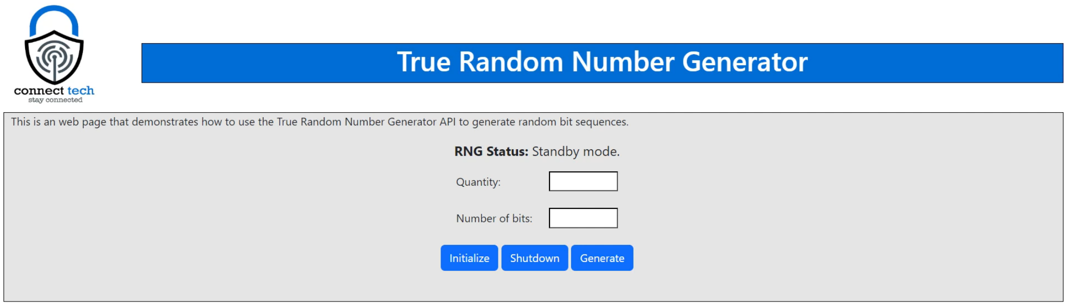
```
curl https://172.16.78.60:5520/trng/randomNum/getRandom?quantity=16numBits=64
```

3. After you recieved your random bits it is possible to put the TRNG into standby mode by sending the following request:

```
curl https://172.16.78.60:5520/trng/randomNum/shutdown
```

2.3 Frontend

In order to have an easy access and control for the REST API, we have got as requirement to implement a frontend webpage. Accordingly, we have developed and implemented a user-friendly interface in order to access and interact with the REST-API´s functionalities.



This is an web page that demonstrates how to use the True Random Number Generator API to generate random bit sequences.

RNG Status: Standby mode.

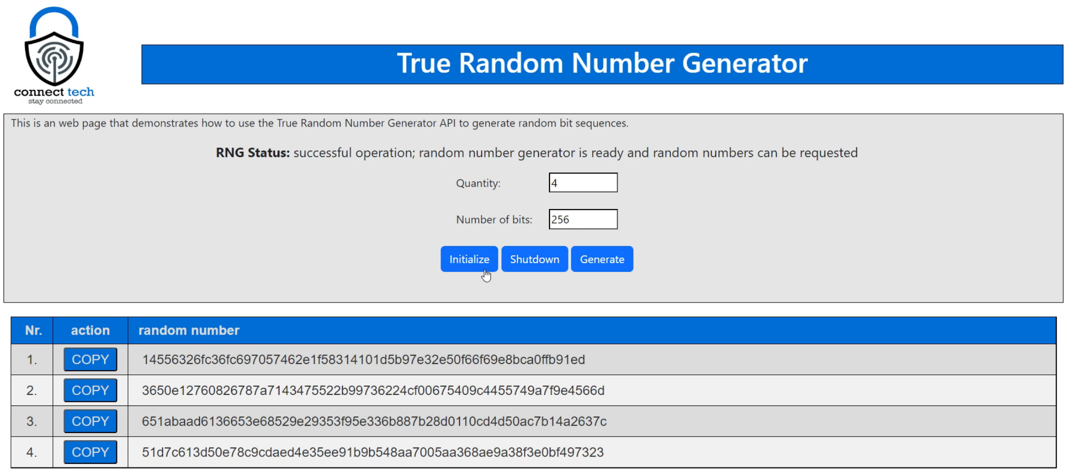
Quantity:

Number of bits:

Figure 1: Webpage

- **Quatity:** This text box is intended for specifying the desired number of bits to be generated. It only accepts positive numbers as input.
- **Number of bits:** This text box is for specifying the length of the bits to be generated. It only accepts positive numbers as input.
- **Initialize:** This button is responsible for the aforementioned init request. Once the button is clicked, it will initialize the pendulum and its associated components.
- **Shutdown:** This button is responsible for the aforementioned shutdown request. Once the button is pressed, it will shut down the pendulum and its associated components.
- **Generate:** This button is responsible for initiating the getRandom request mentioned earlier. When the button is clicked, bits will be generated based on the input from two text boxes. The user can specify the desired number of bits and their desired length. Once the bits are generated, they will be displayed in a table format.

The RNG Status text provides the current state of the pendulum, indicating whether it is initialized, shut down, or generating bits.



True Random Number Generator

This is an web page that demonstrates how to use the True Random Number Generator API to generate random bit sequences.

RNG Status: successful operation; random number generator is ready and random numbers can be requested

Quantity: 4

Number of bits: 256

Nr.	action	random number
1.	COPY	14556326fc36fc697057462e1f58314101d5b97e32e50f66f69e8bca0ffb91ed
2.	COPY	3650e12760826787a7143475522b99736224cf00675409c4455749a7f9e4566d
3.	COPY	651abaad6136653e68529e29353f95e336b887b28d0110cd4d50ac7b14a2637c
4.	COPY	51d7c613d50e78c9cdaed4e35ee91b9b548aa7005aa368ae9a38f3e0bf497323

Figure 2: Webpage - Output example

3 Troubleshooting

Component	Problem	Solution
Magnet	Sliding contacts lost connection	Push contacts back on the tracks
	Sliding contact is defect	Exchange sliding contact
	Cable from Magnet to sliding tracks is defect	Glue back cable onto tracks
	Power supply is defect	Exchange power supply
	Lifting magnet is defect	Exchange magnet
Relay	Relay is defect	Unscrew cables and screw them back into place
		Check connection between relay and Raspberry Pi
Motor	Cables are loose	Reconnect cables
	Strap is broken	Exchange strap
	Strap is not in place	Put strap back in place
	None of the above worked	Check connection between relay and Raspberry Pi
		Check power source
		Exchange motor
Pendulum	Pendulum arm is broken	Exchange with 3D printed arm
Camera	No connection	Check cable on Raspberry Pi and on camera
		Exchange camera