CESGA

Centro de Supercomputación de Galicia

QRNG – Quantum Random Number Generator

15/12/2023

Carlos Mouriño

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA SEGUNDA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

INDICE

Aplicaciones de la aleatoriedad

Tecnologías de generación de aleatoriedad

QRNG

- Web
- Uso
- Ejemplo
- Acceso

Aplicaciones de la aleatoriedad

Muchos problemas computacionales se basan en procesos estocásticos -> requieren gran cantidad de números aleatorios

Los números aleatorios son la base de la seguridad y la privacidad de cualquier comunicación electrónica

Aplicaciones en Seguridad, criptografía, computación

- Ciberseguridad.
- Criptografía y firma electrónica.
- Cálculo científico-técnico: Monte Carlo, optimización, etc.
- Ordenación de listas.
- Sorteo, confiable e imprevisible.

Tecnologías de generación de aleatoriedad

Generadores de números pseudoaleatorios y/o cuasi-aleatorios

- Basados en algoritmos (ampliamente conocidos)
- Son predecibles
- Pueden usar fuentes externas para aumentar entropía: hora del sistema, movimiento ratón, tráfico de red, etc.

Generadores de números aleatorios verdaderos y generadores de números de aleatorios cuánticos

- Basados en fenómenos físicos
- No se pueden predecir
- Las partículas subatómicas son impredecibles

QRNG

Quantum Random Number Generator

FMC 400 Prototyping kit

Basado en la tecnología QRNG de difusión de fase (patentada por Quside)

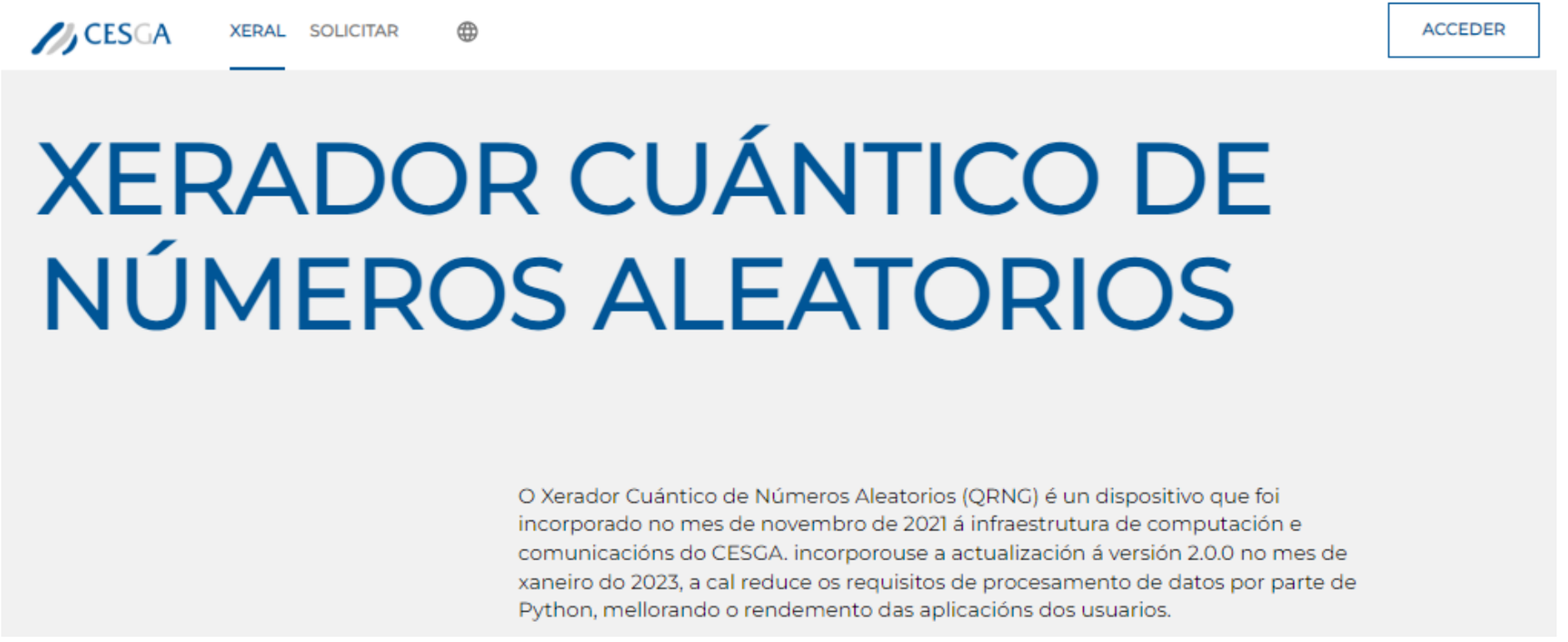
Permite generar secuencias binarias aleatorias:

- Entropía típica de al menos 0,94
- Tasa de aleatoriedad sin procesar de 400Mb/s
- Ratio de salida de bit aleatorios de 100Mb/s

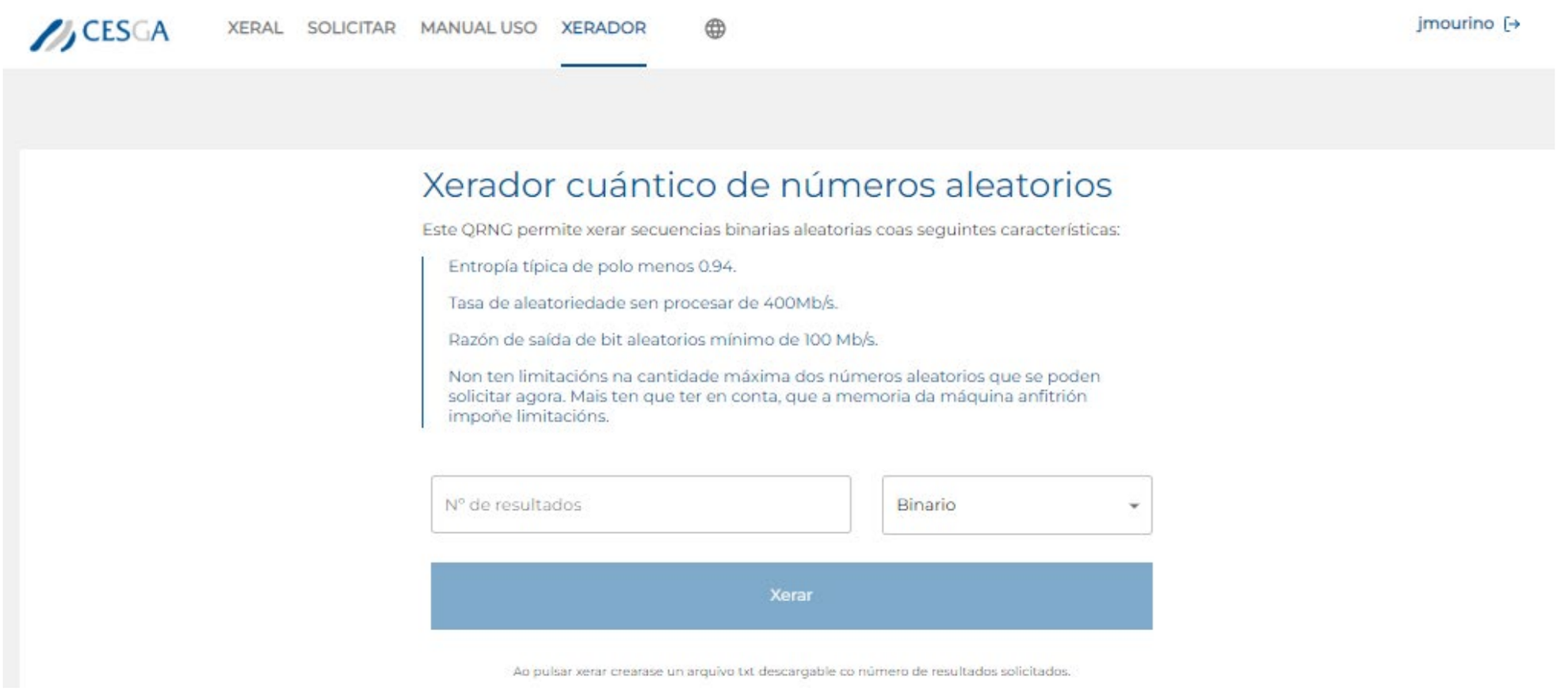
Dispone de una API REST para acceso.

QRNG

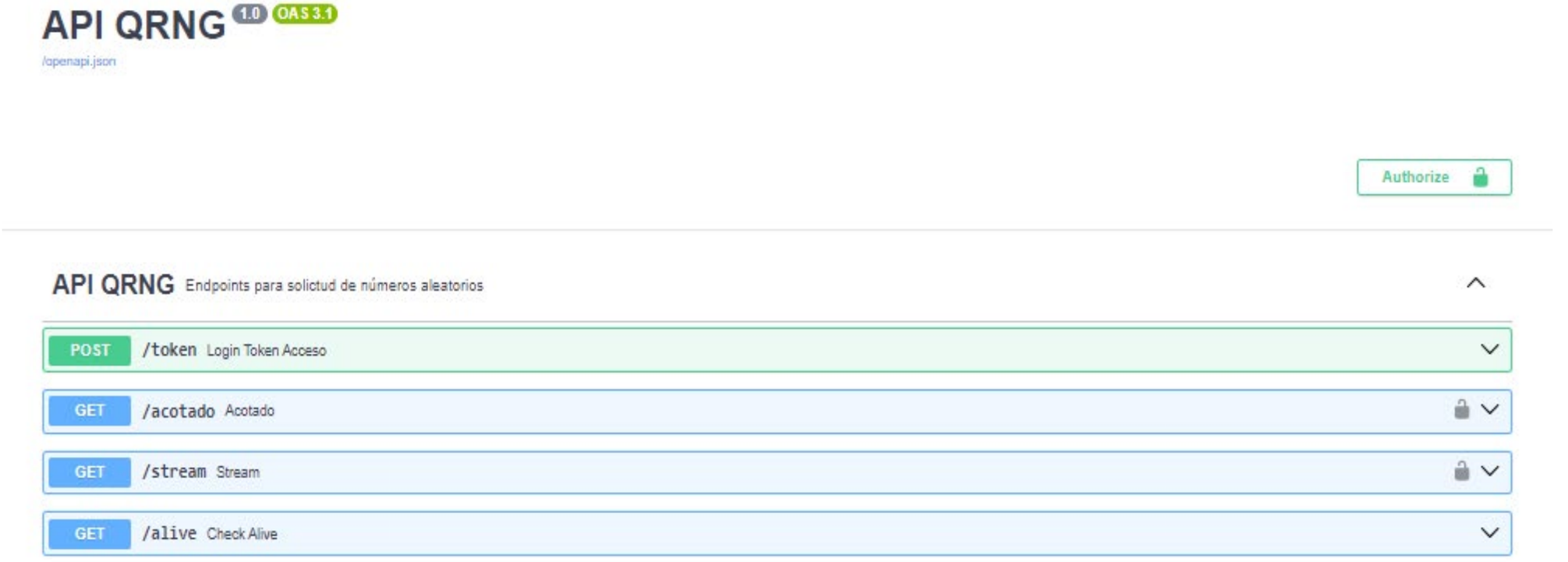
http://qrng.cesga.es/



QRNG – Generador Web



QRNG – API



http://qrng.cesga.es:8000/docs

Uso QRNG

Cargar módulo api_qrng/1.1

Importar a clase ApiQrng

- "url“ IP de la máquina
- "puerto“ Puerto donde se ejecuta el servizo

Generar token de acceso -> ApiQrng.get_token()

- "usuario" Nombre de usuario
- "password" contraseña

Solicitar números -> ApiQrng.acotado() y ApiQrng.stream()

- "paquete" Cantidad de números (por defecto 50) máximo 1000
- "tipo_num" Tipo de número (0 binario, 1 entero, 2 float32, 3 float64)
- "timeout" Tiempo de espera máximo de la petición

http://qrng.cesga.es/userManual

Uso QRNG - Ejemplo

```python
#! /usr/bin/env python
from api_qrng import ApiQrng
import time

test = ApiQrng('qrng.cesga.es', 8000)

### Completar con las credenciales de usuario!
ft3user = 'FT3 user'
ft3pass = 'FT3 pass'
test.get_token(ft3user,ft3pass)

if test.token is not False:

    print("Logged into the QRNG!")

    # Descargamos paquete de 100 números de tipo 2 (float, single precision)
    datos_acotados_2 = test.acotado(tipo_numero=2, paquete=100)
    if datos_acotados_2:
        print("Total de datos acotados 2 ",datos_acotados_2," del tipo ",type(datos_acotados_2[0]))
        print("======================")
        time.sleep(5)

    # Abrimos un stream de generación de números de tipo 1 (enteros) durante 20 segundos
    datos = test.stream(tipo_numero=1,timeout=20)
    for dato in datos:
        print(dato.decode())
```

/opt/cesga/job-scripts-examples-ft3/API_QRNG/

Uso QRNG - Ejemplo

```
[jmourino@login210-19 QRNG]$ python test_api_qrng.py
Logged into the QRNG!
Total de datos acotados 2  [0.3227740526199341, 0.6698432564735413, 0.013383150100708008, 0.834866344928
7415, 0.1729498952627182, 0.008832814171910286, 0.021506471559405327, 0.7179721593856812, 0.053757641464
47182, 0.11912573128938675, 0.9777578115463257, 0.3140181601047516, 0.6506920456886292, 0.72889101505279
54, 0.9242717623710632, 0.3131248354911804, 0.8156806826591492, 0.3299790322780609, 0.6313348412513733,
0.4899435341358185, 0.6563676595687866, 0.2537387013435364, 0.7994868755340576, 0.9599204063415527, 0.17
02853888273239, 0.31002840399742126, 0.4434625804424286, 0.7077199220657349, 0.5378174781799316, 0.60809
21292304993, 0.070448137819767, 0.44721174240112305, 0.6977065205574036, 0.7793321013450623, 0.240125164
3896103, 0.42466050386428833, 0.5726327896118164, 0.009366183541715145, 0.9535510540008545, 0.9500761032
104492, 0.34912076592445374, 0.9304900765419006, 0.7880513668060303, 0.09859021753072739, 0.811231136322
0215, 0.14371900260448456, 0.25590723752975464, 0.33834871649742126, 0.5889732241630554, 0.4587710201740
265, 0.3895791471004486, 0.39125192165374756, 0.5612034201622009, 0.4240872263908386, 0.9483069181442261
, 0.3988202214241028, 0.08836312592029572, 0.7266087532043457, 0.6218149662017822, 0.5502588152885437, 0
.3906088173389435, 0.0688382163643837, 0.18363916873931885, 0.6801163554191589, 0.4251164197921753, 0.14
886802434921265, 0.8729192018508911, 0.4173024296760559, 0.22600141167640686, 0.32828208804130554, 0.329
3530344963074, 0.3893373906612396, 0.7162905335426331, 0.674826443195343, 0.37357428669929504, 0.4294541
4781570435, 0.3759172260761261, 0.03448827564716339, 0.7468849420547485, 0.7623646855354309, 0.938379466
5336609, 0.9461557269096375, 0.14606209099292755, 0.35554733872413635, 0.4767993688583374, 0.71572220325
46997, 0.36511945724487305, 0.6841963529586792, 0.15959100425243378, 0.06208699569106102, 0.998406350612
6404, 0.9594252109527588, 0.26896384358406067, 0.19752614200115204, 0.10011760145425797, 0.8774957656860
352, 0.04719533771276474, 0.8047960996627808, 0.2368742674589157, 0.889771044254303]  del tipo  <class '
float'>
====================
573761737
3139923228
2105498878
```

Acceso QRNG

Se gestiona siguiendo las políticas y procedimientos aplicados en el CESGA para sus infraestructuras de cálculo y almacenamiento.

Usuario CESGA ➡ solicita el acceso a este sistema

No Usuario ➡ solicita cuenta y luego acceso

En la solicitud incluir **breve descripción** de lo que se quiere hacer.

- Entidad y/o investigador responsable.
- Breve descripción del objetivo del proyecto.
- Duración prevista del acceso.
- Fecha inicial solicitada para o acceso.

La memoria puede ser enviada a aplicaciones@cesga.es

http://qrng.cesga.es/request

Acceso QRNG

Informe final al finalizar con los resultados

Agradecimiento en publicaciones

“Trabajo desarrollado gracias al acceso concedido por el Centro de Supercomputación de Galicia a la infraestructura basada en tecnologías cuánticas de la información que permita impulsar la I+D+I en Galicia. Esta infraestructura fue financiada por la Unión Europa, a través del FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER), como parte de la respuesta de la Unión a la pandemia de la COVID-19”

¿Casos de uso? ¿Posibles utilidades?

CESGA

AXENCIA GALEGA DE INNOVACIÓN

UNIÓN EUROPEA

Xacobeo 21·22

CESGA
Centro de Supercomputación de Galicia

DESPREGAMENTO DUNHA INFRAESTRUTURA BASEADA EN TECNOLOXÍAS CUÁNTICAS DA INFORMACIÓN QUE PERMITA IMPULSAR A I+D+i en GALICIA

Apoiar a transición cara a unha economía dixital

Operación financiada pola Unión Europea, a través do FONDO EUROPEO DE DESENVOLVEMENTO REXIONAL (FEDER), como parte da resposta da Unión á pandemia da COVID-19

PROGRAMA OPERATIVO
FEDER GALICIA
2014-2020

Unha maneira de facer Europa

Carlos Mouriño

jmourino@cesga.es

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"