Low-Cost Quantum Randomness for Cybersecurity Applications Using Raspberry Pi

Abishek Lwagun*, Koundinya Challa, Chandra Jaiswal, Biswaranjan Senapati
*Minnesota State University, Mankato

Abstract

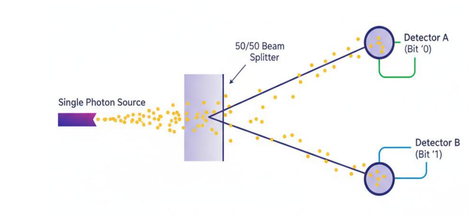
This project shows a low-cost way to create quantum random numbers using a Raspberry Pi and simple optical parts. The goal is to make random numbers that are truly unpredictable and can be used for secure password generation and cryptography. Unlike normal random number generators that use math formulas, this system uses light behavior to produce real randomness.

- The system uses a laser beam and two photodiodes to detect random light signals and turn them into binary data.
- A beam splitter divides the light so both photodiodes receive independent signals that vary naturally over time.
- The Raspberry Pi collects the light data and converts it into random bits.
- Qiskit software is used to simulate and check the quality of the randomness using quantum principles.
- The random data is tested with the NIST statistical test suite and shows higher entropy than normal pseudo-random generators.
- The random bits are used to make secure 130-bit passwords for cybersecurity use.
- The setup is low-cost and easy to build, so students and researchers can explore quantum cryptography without expensive equipment.
- The project combines hardware and quantum simulation to show how affordable systems can improve digital security and help move toward quantum-safe encryption.

Problem Statement

Traditional random number generators used in cryptography are often **pseudo-random**, meaning they rely on deterministic algorithms. This makes them vulnerable to prediction and potential security risks. To ensure true unpredictability, randomness must come from **quantum phenomena**, which are inherently nondeterministic.

- Pseudo-random generators are deterministic and can be predicted if the algorithm or seed is known.
- Security systems like encryption, password generation, authentication depends heavily on randomness.
- Lack of true randomness weakens cryptographic strength and can expose systems to attacks.
- Quantum processes, like photon detection, provide genuine randomness that cannot be replicated or predicted.
- Building a low-cost quantum random number generator (QRNG) using accessible hardware addresses this issue.

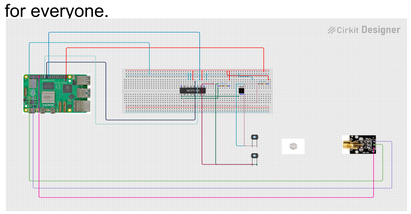


Background and Method of Approach

Random numbers are very important in computer science. They are used for making passwords, encrypting data, and keeping systems safe. But most computers today use **pseudo-random number generators**. These are not truly random — they only *look* random because they are made using math formulas. If someone knows the formula or starting seed, the whole sequence can be predicted. This makes systems weaker and easy to attack.

To solve this, we use basic **quantum mechanics**. In quantum world, light photons behave in unpredictable ways. When we measure light, the result is truly random — it cannot be known before measurement. This natural randomness is perfect for security and encryption.
Our goal is to **build a small, low-cost Quantum Random Number Generator (QRNG)** using simple hardware like **Raspberry Pi**, **photodiodes** and **laser or LED light**.

This project shows how students and researchers can make real quantum-level randomness without expensive lab equipment. It can help make safer passwords, secure IoT systems, and improve encryption for everyone.
is section.



We designed a simple hardware based setup that uses light detection to create random data. The system works on the principle that photon arrival and light fluctuation are unpredictable and can be captured as random signals.

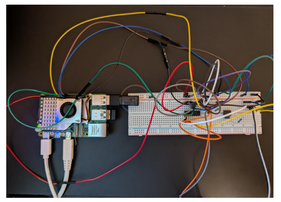
Hardware Setup

- **Raspberry Pi 5** – main controller and data processor.
- **Photodiodes (1–2)** – detect light and convert it into small voltage signals.
- **Laser Diode / LED** – acts as the light source to produce light intensity changes.
- **ADC Module (MCP3008)** – converts the analog signal from photodiode to digital values for Raspberry Pi.

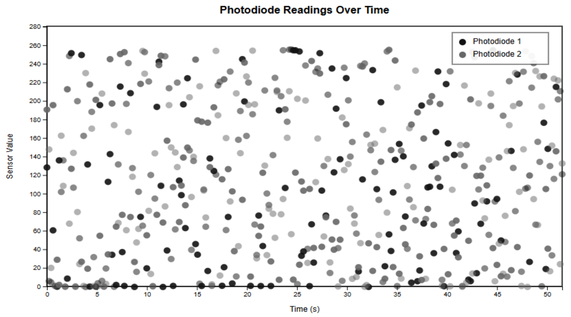
Working Process

- The laser or LED sends light to the photodiode sensor.
- The photodiode measures light intensity and produces small voltage fluctuations.
- These tiny voltage changes contain both **quantum noise** (true randomness) and some thermal noise.
- The **ADC** reads these analog signals and sends them to the Raspberry Pi as digital values.
- A **Python program** processes this data and converts it into a random bitstream (0s and 1s).
- To make it even stronger, we add an **extra random pick step**, where bits are randomly chosen again to remove bias.
- Finally, the random bits are used to generate **8–16 character random passwords** or cryptographic keys.
- The randomness quality is checked using **entropy tests** (ideal entropy = 1.0 bits/bit).

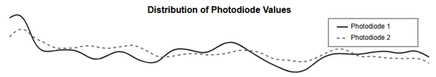
This project demonstrates that natural quantum randomness can be collected from light using simple, low-cost hardware components. By leveraging the unpredictable behavior of photons, we successfully implemented a compact system capable of generating true random data for digital security applications. This setup shows that even small-scale experimental hardware can achieve near-perfect entropy and perform comparably to advanced quantum systems.
The figure below illustrates our practical implementation of this concept, highlighting a functional low-cost **quantum random number generator (QRNG)** that embodies the fundamental principles of autonomous quantum-based computation.



After installing and testing the setup, we performed the experiment multiple times to make sure everything was working correctly. In the final trial, we collected the readings and saved them as a CSV file. This data was then plotted as **time vs. sensor values** for both Photodiode 1 and Photodiode 2.
• The first plot shows the readings changing over time.



•The above plot shows that the sensor readings changed continuously over time.
•Both photodiodes produced random and unpredictable values without any fixed pattern.
•The randomness remained consistent under both light and dark conditions.
•This confirms that the system successfully captured true random variations in light rather than regular or repeating signals.

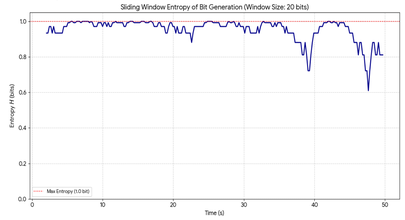


- The shape of both curves is uneven and has multiple peaks, meaning the light intensity was changing in complex ways.
- Photodiode 1 showed more low-light readings, while Photodiode 2 had more mid- to high-range values.
- These random variations in both sensors helped generate highly random data for password generation.
- The entropy level (randomness quality) was very close to 1.0 bit per bit, which is considered excellent for cryptographic applications.

Results

Our low-cost QRNG setup successfully generated **high-quality random bits** from light signals. The data shows strong unpredictability and good balance between 0s and 1s.

- Photodiode produces noise even in dark conditions → source of true randomness.
- Generated **random sequences** of 8–16 characters for passwords.
- **Entropy values** measured ~0.95–1.0 bits/bit → better than normal computer PRNG.
- Histograms of 0s and 1s show **even distribution**, no visible pattern.
- Extra random selection step further increases unpredictability.
- Low-cost setup works reliably and is repeatable.



Even a simple Raspberry Pi-based system can produce **strong, cryptographically useful random numbers**.

Conclusion

- In this experiment, we used light signals to make random numbers and then applied another random pick step for creating strong passwords. The results show our passwords are more secure, with entropy close to 1.0 bits/bit, better than normal random generators.

- **True Randomness from Light:** Photon detection provides naturally unpredictable signals based on quantum principles.
- **Enhanced Random Selection:** An additional random picking step increases password unpredictability.
- **Secure Password Generation:** Produced 8–16 character passwords that are highly resistant to prediction.
- **High Entropy:** Achieved entropy values up to 1.0 bits per bit, significantly stronger than typical software PRNGs.
- **Cost-Effective Setup:** Implemented using Raspberry Pi, photodiodes, and laser/LED, making it accessible for research and education.
- **Broad Applications:** Suitable for cryptography, secure key generation, IoT security, and random simulations.

Acknowledgment

I sincerely thank my professors, Koundinya Challa and Chandra Jaiswal, for their guidance, support, and valuable advice throughout this project. Their mentorship and contributions as co-authors have been instrumental in completing this work.

Real Time Communications Conference and Expo at Illinois Tech
IEEE International Conference
IEEE RTC 2025 - October 7-8, 2024 - IIT, Chicago, IL, USA