Gabriel Manzano

COMS 2302-015

9/30/2025

Random Number Generation

GP: To inform

SP: To inform the audience about Random Number Generation

MI/Thesis: Random numbers in the past have used more predictable methods to create #'s, which could be exploited by users to control the number or predict it, like in pokemon to manipulate the outcomes, or maliciously to get past security that relies on random numbers, so a more secure method to generate #'s, called quantum number generation, allows random #'s to be generated more randomly.

Organization pattern: Chronological

Introduction

1. Attention getter: Have you ever gotten a verification code you did not request? What if I could predict that code and hack into your account?
2. Credibility Statement: Hello, my name is Gabriel Manzano and I have been curious about the inner workings of computers, and manipulating their perceived randomness.
3. Motivation to listen: After this speech, you will have learned how the smart people who design these systems (hopefully) prevent security
4. Thesis: The old way that machines would generate randomness is not very secure because if we could recreate the same environment, the outcome is always the same, which could lead to possibilities of manipulation or prediction and therefore security breaches, so now researchers have found even better ways to create random numbers such as quantum number generation.

Body

1. Old rng methods, such as prng and physical rng, and their weaknesses
    a. ID Quantique - “Computers are deterministic systems. given a certain input, a program will always produce the same output.”
    b. Forms of rng such as pseudo rng and physical rng
    c. Drawbacks of those forms of rng

This poor random number generation can be bad though

2. Main point 2: Why poor rng is bad
    a. This can pose security risks – 6-digit code verification
    b. Lottery and slots - According to a Bradenton Herald article from 2017, Russian hackers were able to reverse engineer a slot machine and effectively cheat by spinning at the exact right moment, as they also use prng

Well, how can we combat these weaknesses

3. Quantum rng, a solution to give true randomness
    a. Quantum random number generation is typically a quantum thing that is truly random
    b. According to a Nature journal on Quantum information from 2016 on Quantum Random Number Generation, Other new methods that have been implemented are light going through a semi-transparent mirror or splitting a light beam along 2 paths and reading either path as either a 1 or a zero

“In conclusion…”

Conclusion

1. Pseudo random number generation and physical number generation are great, but have their faults, leading to possible exploits, which is why people have developed methods of quantum random number generation, which, so far as we know, is completely random.
2. Next time you are sent your 6-digit verification code, appreciate the work that went into making sure it was truly random.

Sources

ID Quantis white paper:

quantique, id. (2020, May). *What is the Q in QRNG?*. what is the Q in QRNG_White Paper.pdf. https://dvd.ilphotonics.com/Id%20Quantique%20-%20fiber-coupled%20detectors%20-%20electronics%20-%20fiber-coupled%20lasers/Electronics/True%20Random%20Number%20Generators/QRNG_Misc/What%20is%20the%20Q%20in%20QRNG_White%20Paper.pdf

npj Quantum Information article:

Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. (2016). Quantum random number generation. *Npj Quantum Information*, *2*(1). https://doi.org/10.1038/npjqi.2016.21

Bradenton Herald article:

Garvin, G. (2017, April 29). Who is mightier, the one-armed bandits or the cellphone bandits? *Bradenton Herald*. Retrieved October 1, 2025, from https://www.bradenton.com/news/local/article147611429.html.