What is randomness? How to generate random numbers?

Berkay Döner/2017400117

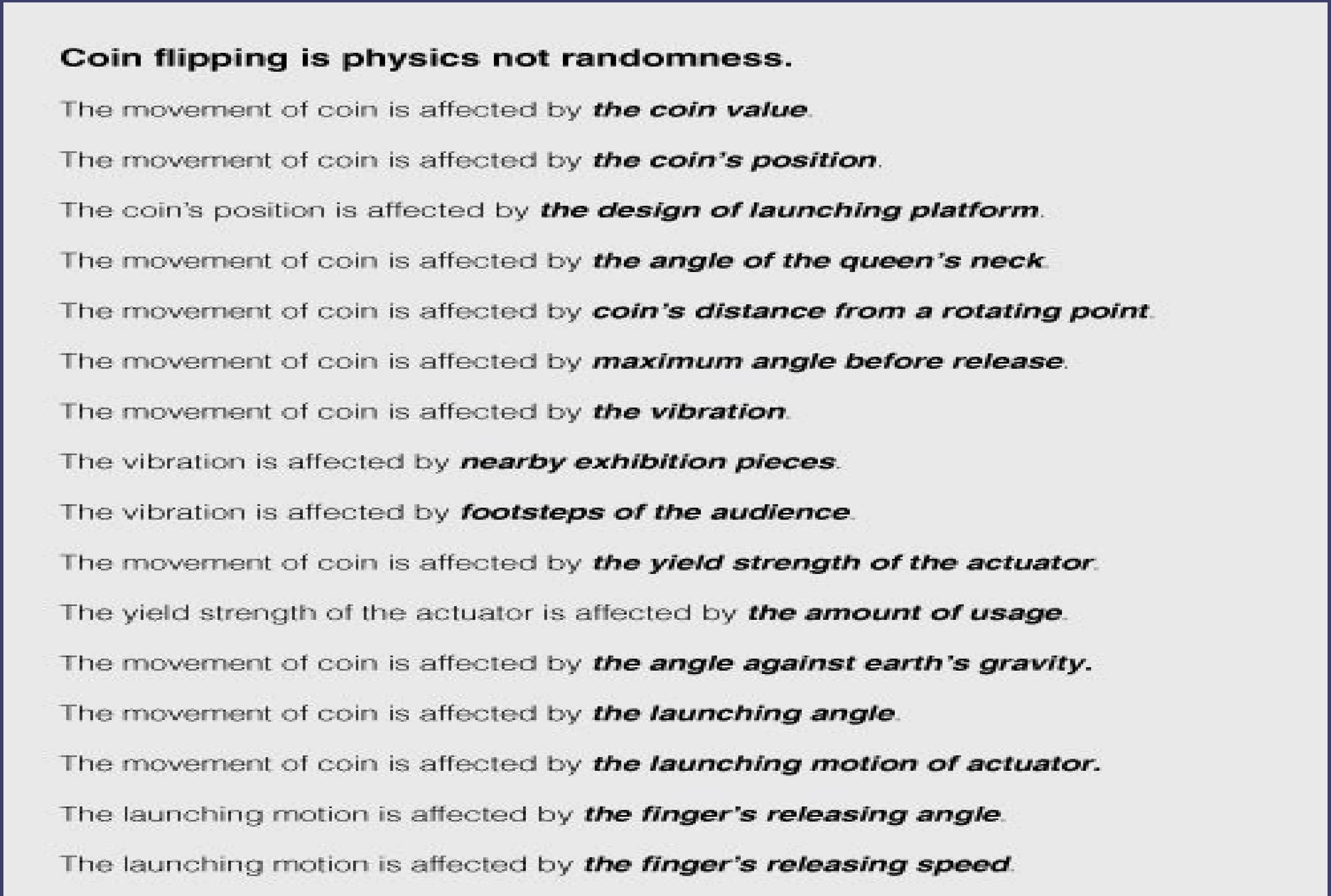
Randomness is the lack of pattern or predictabilit y in events.

A random process has no order and does not follow an intelligible pattern or combination.

Is tossing a coin random?

Is rolling a die random?

They do seem to be predictable by considering the present physical forces and the initial conditions.



Coin flipping is physics not randomness.

The movement of coin is affected by ***the coin value***.

The movement of coin is affected by ***the coin's position***.

The coin's position is affected by ***the design of launching platform***.

The movement of coin is affected by ***the angle of the queen's neck***.

The movement of coin is affected by ***coin's distance from a rotating point***.

The movement of coin is affected by ***maximum angle before release***.

The movement of coin is affected by ***the vibration***.

The vibration is affected by ***nearby exhibition pieces***.

The vibration is affected by ***footsteps of the audience***.

The movement of coin is affected by ***the yield strength of the actuator***.

The yield strength of the actuator is affected by ***the amount of usage***.

The movement of coin is affected by ***the angle against earth's gravity.***

The movement of coin is affected by ***the launching angle***.

The movement of coin is affected by ***the launching motion of actuator.***

The launching motion is affected by ***the finger's releasing angle***.

The launching motion is affected by ***the finger's releasing speed***.

Even though, we could predict the outcome of tossing a coin if we knew the every possible physical phenomena, we don’t know these values precisely.

So, tossing a coin or rolling a dice can be considered random.

Some applications of randomness:

Probability Theory - allows us to measure randomness

Statistics - random data can be used as sample to eliminate bias.

Cryptography - security keys should be generated randomly

Information Theory - noise is random

Pattern Recognition - uses algorithms that use randomness

Finance - stock market prices are seem to be random

So, we need to represent randomness in computers.

How to generate such random numbers on computers?

There are two main approaches:

1-)Hardware random number generators(HRNG)

2-)Pseudo-random number generators(PRNG)

A hardware random number generator is a device that generates random numbers using a physical process. Main physical processes used are:

Shot noise, a quantum mechanical noise source in circuits

Nuclear decay source

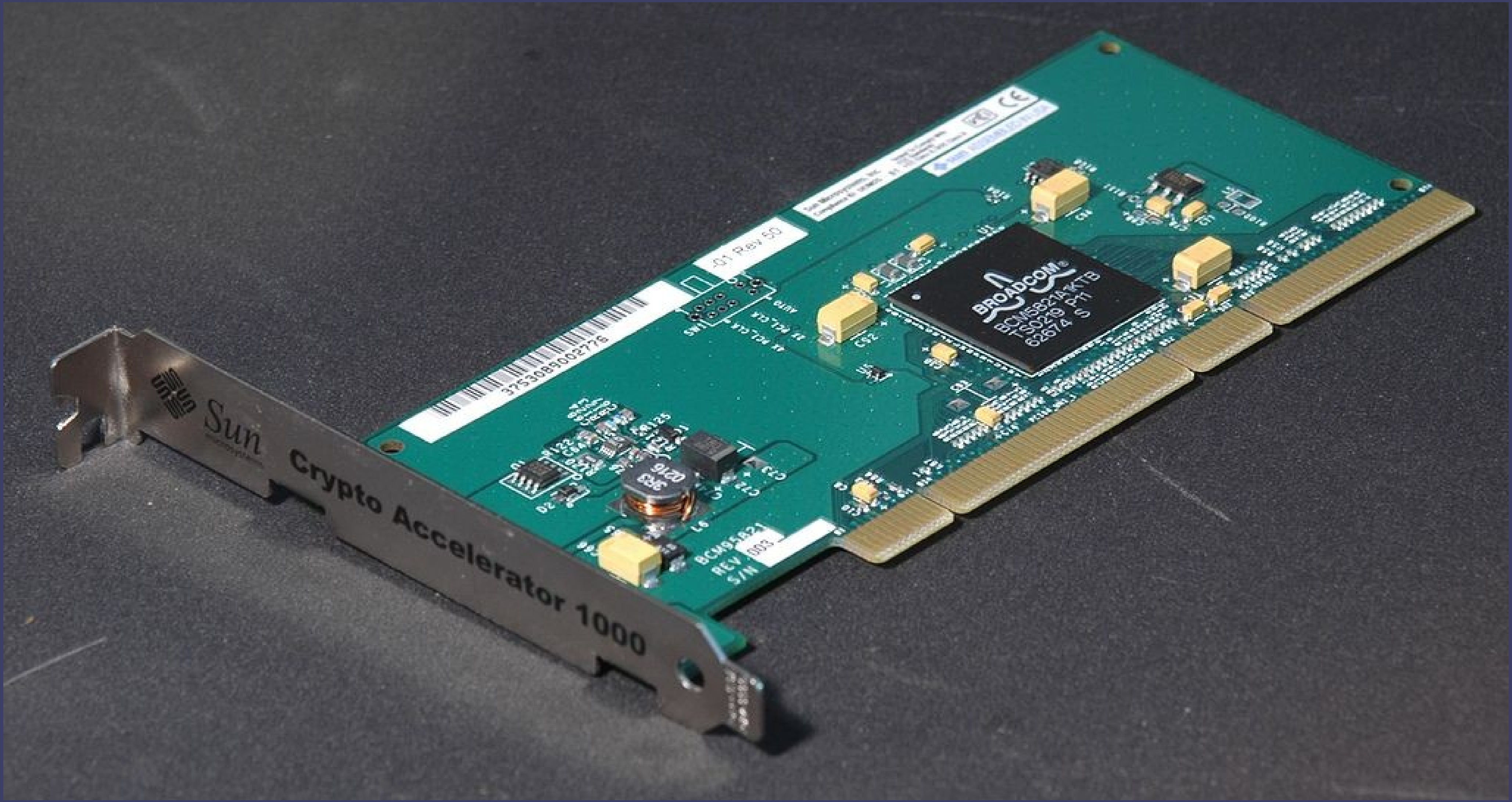
Photons travelling through a semi-transparent mirror

Thermal noise from a resistor

Avalanche noise generated from an diode

Atmospheric noise

Silicon Graphics even developed a HRNG called Lavarand that uses the pictures of a lava lamp and generates random numbers using the patterns of the floating material in the lava lamp.



A computer card with HRNG, used in cryptography

A pseudo-random number generator is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers. Generated numbers seem to be random, in fact, they are not random and can be determined by an initial value called seed.

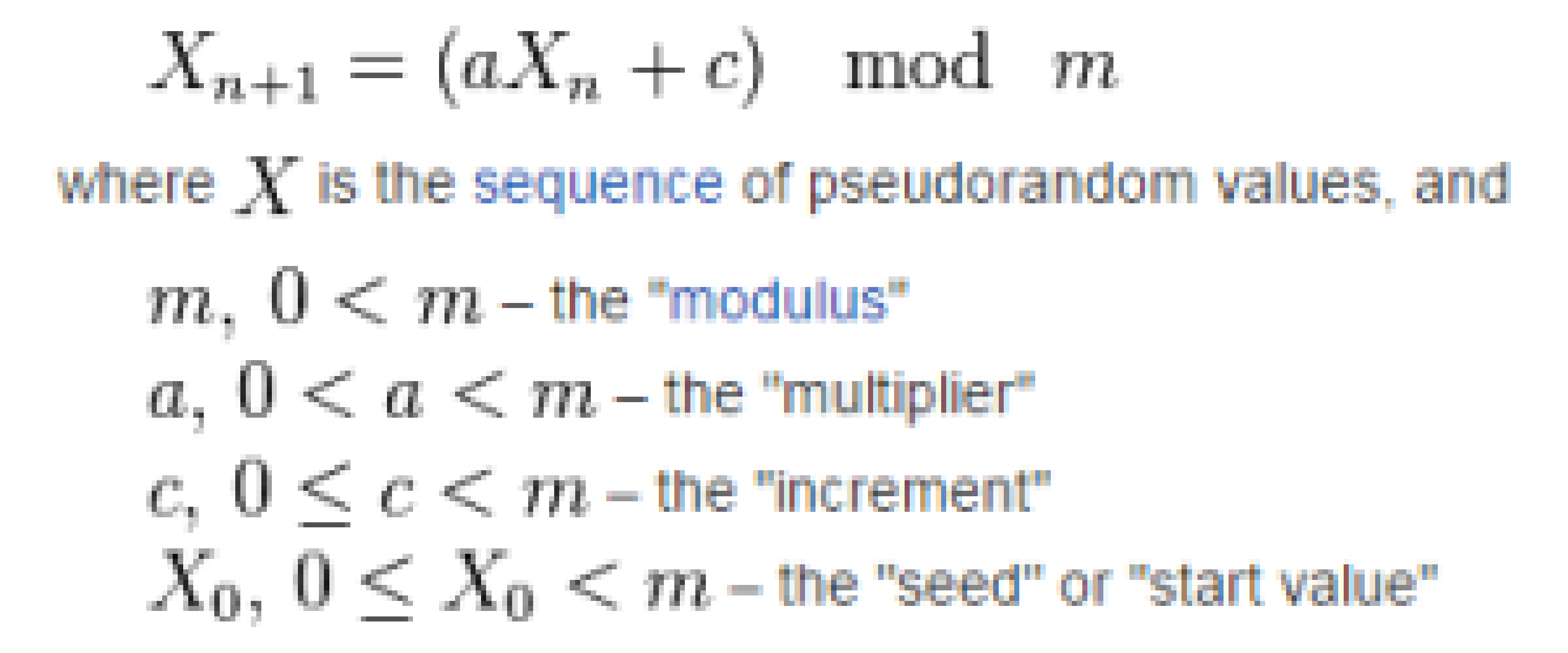
PRNG’s don’t generate true random numbers, but they are preferable for their speed and reproducibility.

If the generated numbers don’t have to be really unpredictable(for applications such as data encryption and gambling), PNGS’s are good enough.

rand() in C++ (srand(seed value) sets the seed)

Random class in Java(new Random(seed) sets the seed)

Linear Congruential Generator is one of the most common and oldest algorithms used for PRNG:



$$X_{n+1} = (aX_n + c) \mod m$$

where X is the sequence of pseudorandom values, and

$m, \ 0 < m$ – the "modulus"

$a, \ 0 < a < m$ – the "multiplier"

$c, \ 0 \leq c < m$ – the "increment"

$X_0, \ 0 \leq X_0 < m$ – the "seed" or "start value"

References:

https://www.random.org/randomness/

https://en.wikipedia.org/wiki/Randomness

https://www.geeksforgeeks.org/pseudo-random-number-generator-prng/

https://en.wikipedia.org/wiki/Hardware_random_number_generator

http://www.dotmancando.info/index.php?/projects/coin-flipper/

https://en.wikipedia.org/wiki/Pseudorandom_number_generator