

Cracking Open Gran Turismo Spec II's Randomizer

Azullia / 0xFC963F18DC21

October 15, 2024

Abstract

Gran Turismo 4 Spec II is a modification for the NTSC-U release of Gran Turismo 4's Online Public Beta. One of its main defining features is a toggleable prize car randomizer, which randomizes what cars one receives as prizes for various actions, picked based on one's in-game username. We will discuss the inner workings of Gran Turismo 4's internal PRNG, and how it is used by Gran Turismo 4 Spec II to generate random prize cars.

Preface

Gran Turismo 4 Spec II is an ISO patch modification for the US soft-release of Gran Turismo 4's Online Public Beta created by TheAdmiester. It brings a lot of additions and changes to the main game, but one of its main draws / features is its prize car randomizer.

Debuting in 2023 as the initial public Randomizer build, the feature was brought into Spec II as a toggleable option. Both versions share the same apparent functionality: changing any prize car¹ into a randomly-selected option based on one's in-game username and the circumstances that one is winning a car in.

As with a lot of other randomizer-adjacent modifications for games, of course, there will be people who wish to know how it internally works, so as to:

- Find an optimal seed to route through.
- Have a really fun or overpowered seed to play through.
- Have an intentionally bad seed as a challenge.

And many more possible reasons. As a disclaimer however, the method described within this paper does not work with the original public Randomizer build from 2023.

Pseudorandom Number Generators (PRNGs)

With most if not all kinds of “randomness” that occurs in computer programs, they are never *truly* random, as that is antithetical to how computers work (i.e. by following instructions in a sequence). Without external inputs of data², computers cannot ever truly replicate something that is truly and irrefutably random³.

¹Prize cars are awarded by Gran Turismo 4 typically for completing all tests in a License grade with Bronze, Silver or Gold level times, winning all races in a single-race event, winning the overall championship of a championship events, completing sets of Driving Missions, etc..

²Cloudflare does something cool for their secure random number generators involving some lava lamps (<https://www.cloudflare.com/en-gb/learning/ssl/lava-lamp-encryption/>), for example.

³By *truly* random, this means that any output is completely unaffected by any surrounding state or previous and future inputs or outputs.

Keeping that in mind, most if not all computer programs use things called *Pseudorandom Number Generators*. As their name suggests, they merely “fake” or “mimic” true randomness, and are not actually truly random. Typically, these take the form of functions of the form:

$$\text{PRNG}(\text{state}) := (\text{pseudorandom output}, \text{new state})$$

And random numbers are generated by repeatedly feeding in the new state⁴ as the next inputs to the PRNG algorithm. The pseudorandom output can then be used in any way the programmer sees fit in order to generate “random”-looking values.

Gran Turismo 4’s PRNG Algorithm

Gran Turismo 4’s main exposed interface for pseudorandom number generation is `MRandom`. This is a class exposed in `Adhoc`⁵ that is used in all places where Gran Turismo 4 requires random-looking values⁶.

MRandom

`MRandom` tracks a simple state: a single unsigned 32-bit integer (which represents a whole number between 0 and 4294967295 inclusive). This state is then fed into its PRNG function inside, which outputs and stores a new state, along with a value that is the “random-looking” value generated alongside. It performs this using a small portion of code inspired by the CRC32 algorithm.

CRC32

The CRC32 algorithm is a checksumming function. Its job is to take a piece of data, and perform some operations to mix groups of bytes in the data together in the order the data comes in. Normally, it can be used as a form of file integrity check (i.e. checking if a file is undamaged / unmodified), but the same property that makes it effective for doing so⁷ also allows it to be a very simple PRNG algorithm.

So how does MRandom work?

Essentially, `MRandom`’s PRNG function looks like the following:

```
def mRandomNext(seed: UInt32): (UInt32, UInt32) = {
  var temp: UInt32 = (17 * seed) + 17
  var result: UInt32 = 0

  for (_ in 0 until 4) {
    val index: UInt8 = result ^ temp
    temp = temp >> 8

    result = (result >> 8) ^ CRC32TABLE(index)
  }

  return (result, (17 * seed) + 17)
}
```

⁴The *state* of a PRNG can be as simple or as complex as it needs to be.

⁵`Adhoc` is a scripting language used by Polyphony Digital for certain tasks in Gran Turismo 4 onwards. See <https://nenkai.github.io/gt-modding-hub/concepts/adhoc/adhoc/> for more information.

⁶The used car dealer uses `MRandom`, for example, to generate the mileages based on the used car cycle week number and car index.

⁷A large cascade effect, where a small change in input makes a large change in output.

It simply operates on 8 bits of the 32-bit integer at a time, calculating a lookup index (that wraps around 0 through 255), that points to a value in a precalculated CRC32 lookup table of values⁸, both using the Exclusive Or⁹ operation.

Although, this doesn't explain how we get useable numbers within a range from these generated pseudorandom values, since without any extra operations, we are stuck with a number anywhere between 0 and 4294967295. This is where the next two functions come in.

GetRange and RandomInt32ToFloat

GetRange wraps around the raw PRNG function to allow it to generate random whole numbers within a range.

```
def getRange(incMin: Int32, excMax: Int32, seed: UInt32): Int32 = {
  val (rval, _) = mRandomNext(seed)
  val multiplier = randomInt32ToFloat(rval)

  // The decimal of the result of the multiplication is chopped off.
  return ((excMax - incMin) * multiplier + incMin)
}
```

RandomInt32ToFloat translates an unsigned 32-bit integer into a decimal value between 0 and 1, where each number between 0 and 4294967295 is translated evenly into that range (with the caveat that 1 is never returned, hence the maximum given in GetRange is exclusive).

Spec II Prize Car Randomizer

In Gran Turismo 4 Spec II, if the prize car randomizer is enabled, when one would normally earn a prize, instead of awarding the prize associated with that instance of a prize, it will randomly select a car from a list of all cars available in Spec II.

How it randomly selects a car is based on the username, the current “trigger” that is giving the prize car, and what type of trigger it is:

- Username is self-explanatory. It is the up to 30-long string one inputs when making a save on a memory card for the first time¹⁰.
- Triggers are a list labels of events that you can win a prize car in, they represent things like event hall events (Sunday Cup, etc.), License grade tiers (B Bronze, etc.) or Mission Set completions (E.g. One-Lap Magic 30-34).
- Types of triggers denote what kind of condition it was activated (an event win, mission set completion, license grade completion, etc.).

These parts are then put together into one big string, and that is then used as the seed whenever one wins a prize (e.g. Username “Foo”, event Sunday Cup (“am_sunday_0000”) and type “win” is put together to become “Fooam_sunday_0000win”). The question is then:

How does it turn that text into a number to feed into GetRange?

⁸The first table in <https://web.mit.edu/freebsd/head/sys/libkern/crc32.c>

⁹https://en.wikipedia.org/wiki/Exclusive_or

¹⁰If entering usernames there, **do not** use the HD HUD / UI texture pack, as that incorrectly blanks out some of the keys on the improved keyboard incorrectly.

Fowler-Noll-Vo Hashes

A hash function is a way to generate a “summary” of a piece of data, similar to a checksum. They also ideally exhibit the same property as a checksum, where a small change in input data creates a massive change in the final hash output.

Gran Turismo 4 Spec II uses a variant of the Fowler-Noll-Vo algorithm, a very simple to implement hashing algorithm, especially for text / strings. Its implementation in Spec II is specifically the FNV-1a variant, which looks like:

```
def fnv1a(str: String): UInt32 = {  
    // These starting values can usually be substituted for other  
    // suitable values in other implementations of FNV-1a.  
    val prime: UInt32 = 16777619  
    var result: UInt32 = 0x811C9DC5  
  
    for (chr in str) {  
        result ^= chr.toUInt8  
        result *= prime  
    }  
  
    return result  
}
```

So the example string such as “Fooam_sunday_0000win” is then passed into fnv1a (which in this case becomes 3244945079), and then the result is passed into GetRange as the seed.

Final Algorithm

Putting it all together, we have the following algorithm:

```
extern val allCars: List[Car]  
  
def randomPrize(username: String, trig: String, trigType: String): Car = {  
    val seed = fnv1a(username + trig + trigType)  
    val index = getRange(0, allCars.length, seed)  
  
    return allCars(index)  
}
```

A very simple algorithm overall, but very effective at its objective of delivering the player random prize cars based on username¹¹, while being able to choose the same car again should a player decide to (e.g.) repeat an event they’ve won a prize car before.

Appendices

Spec II Adhoc Sources

They can be found on TheAdmiester’s GitHub here: <https://github.com/TheAdmiester/OpenAdhoc-GT4SpecII>.

Please be warned that some amount of programming experience will be needed to understand the code, and a primer can be found on Nenkai’s GT Modding hub at <https://nenkai.github.io/gt-modding-hub/concepts/adhoc/adhoc/>

¹¹For cars with multiple possible colours, the seed fed to GetRange is based on the PS2’s system clock.

Analyzer Tool Sources

They can be found at <https://github.com/MF42-DZH/GT4S2RC>.

Seed Bruteforcing

With the possibility to now check the cars found in a seed for Spec II's Randomizer, it becomes possible to look through seeds (many, many seeds) in order to try and find a seed optimised for some purpose.

TeaKanji was and is a major help in this process, providing both approximate “viability” values for all cars in Spec II, and a list of cars that are essential for a 100% run using just prize cars supplied by the randomizer. We've both gone through likely millions of usernames, checking their prizes to see if we can either:

- Find a seed with consistently overpowered car drops.
- Find a seed where it is possible to 100% the game in with just prize cars.

The first goal was achieved relatively comfortably by trying to find seeds with a high average car viability, some examples include:

- GatewomanBoundaries (with its **five** 787Bs!)
- ZaniestDisconcert (with its **B License Bronze** Formula Gran Turismo!)
- [REDACTED AT THE REQUEST¹² OF CERO, PEGI, THE ACB, AND THE ESRB]
- std::reinterpret_cast<float> (with its **five** BMW V12 LMRs!)

The next goal, which we have still not met, is to find a username that is able to 100% the game without any bought cars. The closest we have gotten is five cars needing to be bought for a candidate seed, one such example being “ItDoESn'tHAVEtoBEthiSWaY” (case-sensitive).

Feel free to use the bruteforcers included in the repository (or write your own) to try and attempt to find that mythical 100%-able seed!

Acknowledgements

- **Nenkai**: Disassembly Help and GTHD Debug Executables Archive
- **TeaKanji**: Car Viability Info, 100% Necessities Info, Bruteforcing Script Help
- **beardypig**, **astrelsky**: The ghidra-emotionengine scripts for Ghidra
- **mrxbas**, **Yellowbird**: General Support
- **TheAdmiester**: Creating Gran Turismo 4 Spec II

¹²(at gunpoint)