Package 'ironseed'

August 21, 2025

Title Improved Random Number Generator Seeding

Version 0.2.0

Description A procedure for seeding R's built in random number generators using a variable-length sequence of values. Accumulates input entropy into a 256-bit hash digest or ``ironseed'' and is able to generate a variable-length sequence of output seeds from an ironseed.

License MIT + file LICENSE

Language en-US

Encoding UTF-8

RoxygenNote 7.3.2

Biarch TRUE

NeedsCompilation yes

URL https://github.com/reedacartwright/ironseed

BugReports https://github.com/reedacartwright/ironseed/issues

Suggests tinytest

Author Reed Cartwright [aut, cre] (ORCID: <https://orcid.org/0000-0002-0837-9380>), National Science Foundation DBI-1929850 [fnd]

Maintainer Reed Cartwright <racartwright@gmail.com>

Repository CRAN

Date/Publication 2025-08-20 22:10:01 UTC

Contents

ironseed *Ironseed: Improved Random Number Generator Seeding*

Description

An ironseed is a 256-bit hash digest constructed from a variable-length input sequence and can be used to generate a variable-length output sequence of seeds, including initializing R's built-in random number generator.

- `ironseed()` creates an ironseed from user supplied objects, from external arguments, or automatically from multiple sources of entropy on the local system. It also initializes R's built-in random number generator from an ironseed.
- `set_ironseed()` calls `ironseed()` with set_seed = TRUE.
- `create_ironseed()` constructs an ironseed from a list of seed objects, following the rules described below. `auto_ironseed()` constructs an ironseed from multiple sources of entropy on the local system.
- `is_ironseed()` tests whether an object is an ironseed, and `is_ironseed_str()` tests if it is a string representing and ironseed.
- `as_ironseed()` casts an object to an ironseed, and `parse_ironseed_str()` parses a string to an ironseed.

Usage

```
ironseed(
  ...,
  set_seed = !has_random_seed(),
  quiet = FALSE,
  methods = c("dots", "args", "env", "auto", "null")
)

set_ironseed(
  ...,
  quiet = FALSE,
  methods = c("dots", "args", "env", "auto", "null")
)

create_ironseed(x)

auto_ironseed()

is_ironseed(x)

is_ironseed_str(x)

as_ironseed(x)

parse_ironseed_str(x)
```

Arguments

`...`	objects
`set_seed`	a logical indicating whether to initialize `.Random.seed`.
`quiet`	a logical indicating whether to silence messages.
`methods`	a character vector.
`x`	a string, ironseed, list, or other object

Details

Ironseeds have a specific string representation, e.g. "rBQSjhjYv1d-z8dfMATEicf-sw1NSWAvVDi-bQaKSKKQmz1", where each element is a 64-bit number encoded in little-endian base58 format.

Parameter `set_seed` defaults to `TRUE` if `.Random.seed` does not already exist and `FALSE` otherwise.

Ironseed behaves differently depending on the number of arguments passed as `...` and the value of `methods`. If `...` has a length of zero **and** initialization is disabled, then `ironseed()` returns the last ironseed used to initialize `.Random.seed`. Otherwise, it generates an ironseed from an input sequence according to the methods included in `methods`.

When generating an ironseed, `ironseed()` tries the listed methods starting from the first value and continuing until it can generate an ironseed. If no method works, an error will be raised.

- dots: Use the values passed as `...` to construct an ironseed. Most atomic types and lists of atomic types can be used. `ironseed()` and `ironseed(NULL)` are considered empty inputs and the next method will be tried.
- args: Use command line arguments to construct an ironseed. Any arguments that begins with `--seed=` or `-seed=` will be used as strings, after the argument names are trimmed. If no matching arguments are found, the next method will be tried.
- env: Use the value of the environmental variable "IRONSEED" as a scalar character to construct an ironseed. If this variable doesn't exist or is set to an empty string, the next method will be tried.
- auto: Use multiple sources of entropy from the system to generate an ironseed. This method always constructs an ironseed.
- null: Generate a "default" ironseed using no input. This method always constructs an ironseed.

If the input sequence has one value and it is an ironseed object, it is used as is. If the input sequence is a scalar character that matches an ironseed string, it is parsed to an ironseed. Otherwise, the input sequence is hashed to create an ironseed.

An ironseed is a finite-entropy (or fixed-entropy) hash digest that can be used to generate an unlimited sequence of seeds for initializing the state of a random number generator. It is inspired by the work of M.E. O'Neill and others.

An ironseed is a 256-bit hash digest constructed from a variable-length sequence of 32-bit inputs. Each ironseed consists of eight 32-bit sub-digests. The sub-digests are 32-bit multilinear hashes that accumulate entropy from the input sequence. Each input is included in every sub-digest. The coefficients for the multilinear hashes are generated by a Weyl sequence.

Multilinear hashes are also used to generate an output seed sequence from an ironseed. Each 32-bit output value is generated by uniquely hashing the sub-digests. The coefficients for the output are generated by a second Weyl sequence.

To improve the observed randomness of each hash output, bits are mixed using a finalizer adapted from SplitMix64. With the additional mixing from the finalizer, the output seed sequence passes PractRand tests.

Value

An ironseed. If `.Random.seed` was initialized, the ironseed used will be returned invisibly.

References

- O'Neill (2015) Developing a seed_seq Alternative. https://www.pcg-random.org/posts/developing-a-seed_seq-alternative.html
- O'Neill (2015) Simple Portable C++ Seed Entropy. https://www.pcg-random.org/posts/simple-portable-cpp-seed-entropy.html
- O'Neill (2015) Random-Number Utilities. https://gist.github.com/imneme/540829265469e673d045
- Lemire and Kaser (2018) Strongly universal string hashing is fast. https://arxiv.org/pdf/1202.4961
- Steele et al. (2014) Fast splittable pseudorandom number generators. doi:10.1145/2714064.2660195
- Weyl Sequence https://en.wikipedia.org/wiki/Weyl_sequence
- PractRand https://pracrand.sourceforge.net/

See Also

set.seed .Random.seed

Examples

```
# Generate an ironseed with user supplied data.
# This will initialize an uninitialized `.Random.seed`.
ironseed::ironseed("Experiment", 20251031, 1)

# Generate an ironseed automatically and force initialize
# `.Random.seed` with it.
ironseed::ironseed(set_seed = TRUE)

# Return last used ironseed.
ironseed::ironseed()
```

`ironseed_stream` *Ironseed output seed sequences*

Description

Output sequences of 32-bit seeds are generated from an ironseed using multilinear hashes. The coefficients for these hashes are generated by a different Weyl sequence from the input hashes. A hash finalizer is also used to mix bits and improve observed randomness.

- `create_seedseq()` uses an ironseed to generate a sequence of 32-bit seeds.
- `ironseed_stream()` returns a function that can be used to generate a seed sequence iteratively.

Usage

```
ironseed_stream(..., methods = c("dots", "args", "env", "auto", "null"))

create_seedseq(fe, n)
```

Arguments

`...`	objects
`methods`	a character vector.
`fe`	an ironseed
`n`	a scalar integer specifying the number of seeds to generate

Value

an integer vector containing 32-bit output seeds. If `n` is missing, `ironseed_stream()` returns the underlying ironseed.

See Also

ironseed

Examples

```
# Generate 20 seeds from an ironseed
fe <- ironseed("Experiment", 20251031, 1, set_seed = FALSE)
create_seedseq(fe, 20)

# Create a function that can be called multiple times to produce seeds
get_seeds <- ironseed_stream("Experiment", 20251031, 1)

# generate 10 seeds
get_seeds(10)

# generate 10 more seeds
```

```
get_seeds(10)

# output the ironseed used for the stream
get_seeds()
```

`with_ironseed` *Temporary ironseeds*

Description

`with_ironseed()` runs code with a specific ironseed and restores global state afterwards. `local_ironseed()` restores global state when the current evaluation state ends.

Usage

```
with_ironseed(seeds, code, quiet = FALSE)

local_ironseed(seeds, ..., quiet = FALSE, .local_envir = parent.frame())

with_ironseed_stream(func, code)

local_ironseed_stream(func, .local_envir = parent.frame())
```

Arguments

`seeds`	An object or list of objects suitable for constructing an ironseed.
`code`	Code to execute in the temporary environment.
`quiet`	a logical indicating whether to silence messages.
`...`	Additional objects.
`.local_envir`	The environment to use for scoping.
`func`	A stream function returned by `ironseed_stream()`

Value

`with_ironseed()` returns the results of the evaluation of the code argument. `local_ironseed()` returns the constructed ironseed.

See Also

ironseed ironseed_stream

Index