Package 'Rrdrand'

July 4, 2018

Version 0.1-16

Date 2018-07-04

Title 'DRNG' on Intel CPUs with the 'RdRand' Instruction for R

Author Ei-ji Nakama <nakama@ki.rim.or.jp>, Junji NAKANO <nakanoj@ism.ac.jp>

Maintainer Ei-ji Nakama <nakama@ki.rim.or.jp>

Depends R (>= 3.0.0)

Description Make use of the hardware random number accessed by the 'RdRand' instruction in recent Intel CPUs (Ivy Bridge and later).
'DRNG' is ``Digital Random Number Generator''.

License AGPL-3

SystemRequirements need the RDRAND instruction on Intel CPU. and C compiler must be able to compile a GNU-style in-line assembler.

URL http://prs.ism.ac.jp/~nakama/Rrdrand/

NeedsCompilation yes

Repository CRAN

Date/Publication 2018-07-04 08:10:15 UTC

R topics documented:

`Rrdrand-package` *DRNG(Digital Random Numbers Generate) on Intel CPUs with the RdRand instruction for R*

Description

Make use of the hardware random number accessed by the RdRand instruction in recent Intel CPUs (Ivy Bridge and later).

This library defines the user_unif_rand symbol and gives back a random number of RdRand.

'hasRDRAND' returns either RdRand available by executing the CPUID.

if HasRDRAND return false of library load time, it does not change the RNGkind.

if you do changed RNGkind("user") by manual operation and RdRand is not available, you get NaN.

If you want to detach, it will be set to RNGkind of "default".

Usage

```
hasRDRAND()
```

Details

http://prs.ism.ac.jp/~nakama/Rrdrand

Author(s)

Ei-ji Nakama <nakama@com-one.com> and Junji NAKANO <nakanoj@ism.ac.jp>

Maintainer: Ei-ji Nakama <nakama@com-one.com>

Examples

```
library(Rrdrand)
if(hasRDRAND())
  print(RNGkind())
  print(runif(3))
```

Index