Method to Improve Random Number Generators

Tech ID: 21825 / UC Case 2005-048-0

TECHNOLOGY DESCRIPTION

UC San Diego inventors have come up with a new method for improving pseudo-random number generators. Based on new theoretical achievements in algebraic theory of quasigroups, it can work over alphabets of n-bit letters for every n>1, and can enlarge the period of the pseudo random string of numbers and pass every known statistical test of randomness. The method is easy to implement in software or hardware in less than 1 kilobyte of memory space. The method can also be used as an improver of biased truly random number generators.

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	8,041,031	10/18/2011	2005-048

CONTACT

University of California, San Diego
Office of Innovation and Commercialization
innovation@ucsd.edu
tel: 858.534.5815.

INTRODUCING
UC TechAlerts
New technology matches delivered to your email at your preferred schedule
SEARCH
SAVE SEARCH
Learn More

OTHER INFORMATION

CATEGORIZED AS

- **Computer**
  - Security

RELATED CASES

2005-048-0, 2005-050-0