Title (en)

APPARATUS AND METHOD FOR GENERATING A RANDOM BIT SEQUENCE

Title (de)

VORRICHTUNG UND VERFAHREN ZUM ERZEUGEN EINER ZUFALLSBITFOLGE

Title (fr)

DISPOSITIF ET PROCÉDÉ DE GÉNÉRATION D'UNE SÉQUENCE DE BITS ALÉATOIRES

Publication

EP 2329356 A1 20110608 (DE)

Application

EP 09781262 A 20090730

Priority

- EP 2009059837 W 20090730
- DE 102008048292 A 20080922

Abstract (en)

[origin: WO2010031630A1] An apparatus (1) for generating a random bit sequence (ZZ) comprises a ring oscillator which includes a plurality of inverting digital devices (2-11) and on which an oscillator signal (OS) can be tapped. An intermediate storage element (14) monitors and stores fluctuating levels of the oscillator signal (OS). Furthermore, at least two controllable switch devices (12, 13) for simultaneously exciting at least two harmonic wave edges (OW1, OW2) of the ring oscillator are provided in a signal path of the ring oscillator. The phasing of the two harmonic wave edges (OW1, OW2) and a potential convergence thereof are subject to statistical fluctuations, which are used as a basis for the random bit generation. An apparatus and a method for generating random bit sequences are claimed. A corresponding random number generator can be used in particular as a FPGA for security applications, such as cryptographic methods. The apparatus (1) comprises substantially digital components, which are easy to produce in a standardized manner. A dedicated regulating circuit is not necessary. The apparatus is also robust toward exterior influences. The figures illustrate circuit diagrams of possible implementations and signal curves of the occurring signals.

IPC 8 full level

G06F 7/58 (2006.01); **H03K 3/84** (2006.01)

CPC (source: EP US)

G06F 7/588 (2013.01 - EP US); **H03K 3/84** (2013.01 - EP US); **H04L 9/0861** (2013.01 - EP US)

Citation (search report)

See references of WO 2010031630A1

Cited by

US9891888B2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

Designated extension state (EPC)

AL BA RS

DOCDB simple family (publication)

WO 2010031630 A1 20100325; DE 102008048292 A1 20100408; DE 102008048292 B4 20120712; EP 2329356 A1 20110608; US 2011163818 A1 20110707; US 8410857 B2 20130402

DOCDB simple family (application)

EP 2009059837 W 20090730; DE 102008048292 A 20080922; EP 09781262 A 20090730; US 200913119765 A 20090730