

ZRANDOM USB

Generation of True Random Numbers

User's Guide - Version 2.2

© WESTPHAL ELECTRONIC

Contents

Introduction	2
Fields of Application for the ZRANDOM USB TRNG	2
Advantages of True Random Numbers	2
Physical Background	3
ZRANDOM USB - Package Contents	3
System Requirements	3
Hardware Installation	4
Software Installation	4
Trouble Shooting	6
Terms and conditions of trade / Liability	6
Technical Specifications	7

Introduction

Random numbers are needed for many purposes, the most important applications may be production of key code, encryption of data and Monte-Carlo simulations. In many cases pseudo-random numbers can be used but for some applications the disadvantages of these numbers (deterministic sequences, hidden correlations) are not acceptable. Especially for high security applications non-deterministic (true) random numbers are needed since no unauthorized person should be able to decode encrypted data due knowledge of the used code number algorithm. It is obvious that the same precaution is necessary for commercial applications such as electronic gambling machines. The expanding electronic communication, dominated by the Internet, is the main reason for the rising need of true random numbers. The ZRANDOM USB - TRUE RANDOM NUMBER GENERATOR (TRNG) is a professional device for the production of non-deterministic random numbers. It can be used in combination with almost every IBM-compatible Personal Computer or Notebook. The hardware installation as well as the operation of the software are quite easy. Due to the high generation rates of 70,000 bits/s (physical mode) or 300,000 bits/s (XOR mode) a true random bit production of 721 MByte or 3.1 GByte per day is possible with a 1.7 GHz CPU.

Fields of Application for the ZRANDOM USB TRNG

- Generation of code numbers
- Encryption of data (e.g. for communication in the Internet)
- Direct use for Monte-Carlo simulations
- Test of pseudo-random number generators
- Numeric solution of mathematical problems
- Control/test of gambling machines

Advantages of True Random Numbers

- No periodicities.
- No predictability of random numbers due to preceding sequences.
- Not based on an algorithm. (Data can be encrypted absolutely secure.)
- Certainty that no hidden correlations are present.
- Certainty that the equipartition fluctuations are purely stochastic.
- (Pseudo-random numbers contain systematic, unnatural fluctuations in the equipartition.)

Physical Background

The natural, non-deterministic character of the random numbers produced by the ZRANDOM USB generator is based on a physical process called thermal electronic noise. The noise voltage U_{noise} which originates at a resistance R is

$$U_{noise} \propto \sqrt{T \cdot R \cdot f}$$

with the absolute temperature T and the frequency bandwidth f . By use of a special noise power spectrum and a suitable sampling rate high quality random bits are obtained.

ZRANDOM USB - Package Contents

1. External device (contains noise generator)
2. Standard USB cable
3. Software incl. USB driver (CD ROM)
4. This User's Guide

System Requirements

1. CPU: IBM compatible 300 MHz (1.7 GHz or more recommended)
2. USB connector (USB 1.0 high speed or USB 2.0)
3. VGA graphic display, 16 colors
4. CD ROM drive
5. Hard disk: 2 MB free space for ZRANDOM USB programs
x MB free space for random number files
6. Operating System: Windows 98/ME/2000/XP

Note: The maximum random bit generation rates (70.000 / 300.000) may only be achieved with the recommended hardware.

Hardware Installation

Connect the ZRANDOM USB external device to your Personal Computer or Notebook by use of the USB cable. The external device is supplied by the USB port. You do not need a separate power supply. You can connect the external device everytime, i.e. when the computer is switched on or off.

The LED at the external device indicates that the external device is powered by the USB port.

Set-up of the external device

Although the noise generator in the external device is shielded against electromagnetic radiation with a suppression of more than 75 dB, closeness to strong jammer oscillators should be avoided. In customary offices there are two types of potential sources of jamming signals: computer monitors and switching power supplies. The interference level of such devices drops very quickly with the distance. Keep a minimum distance of 30 cm between such devices and the ZRANDOM USB.

Random bit generation rate

The nominal rate of 70.000 bits per second in the physical mode and 300.000 bits per second in the XOR mode is given for a CPU with 1.7 GHz. On very slow or loaded systems the random bit rate can be significantly lower.

Software Installation

The following instructions presume that you are familiar with your computer and your operating system. Make sure that the ZRANDOM USB hardware is properly installed before any ZRANDOM USB program is executed.

One of the operating systems **Windows 98/ME/2000/XP** can be used.

Create a new directory on your hard disk.

e.g. C:\ZRANDOM

Copy all directories and files from the ZRANDOM CD ROM to the new directory.

Installation of the USB driver

If you connect the ZRANDOM USB external device to your computer for the first time you will be asked for a suitable driver. Insert the ZRANDOM CD ROM. Normally, Windows will find the USB driver files automatically.

Following files need to be in your Windows directories:

```
c:\windows\inf\ezusbw2k.inf
c:\windows\system32\drivers\ezusb.sys
```

(The directory "c:\windows\inf" may be hidden in the Windows Explorer.)

The USB driver files are on the CD ROM in the directory ...*ZRANDOM-USB-Driver*\

Start of generation program

Start the generation program by double click on *ZranUSB.exe* in the directory ...*ZRANDOM-USB*\

You can also create an icon with a link to the file *ZranUSB.exe*.

Random bits will be stored in a binary **.bin* file, and protocol information will be stored in an ASCII **.log* file. If you don't specify a special directory these files will be stored in the same directory as *ZranUSB.exe*.

Warning:

Avoid usage of task manager or other programs during random bit generation.

Conversion of binary random bit files to decimal random numbers

Start the conversion program by double click on *Zconvert.exe* and select suitable conversion parameters. The converted integer or real true random numbers will be stored in an ASCII **.asc* file.

The programs are almost self-explaining. After the start button is pressed, a binary file (default file name *ZZ_000.BIN*) will be created. In a related protocol file (default name *ZZ_000.LOG*) you will find all relevant data concerning the generation. All settings (white edit fields) will be stored in the parameter file **.PAR* before you exit the program. Usually REAL or INTEGER random numbers are needed. You can convert binary random bit files to ASCII random number files by use of *Zconvert.exe*. In this program you can select the type of random number (INTEGER or REAL) and the number of bits per random number. In addition you can choose the separator between the random numbers. Then an ASCII file (default name *ZZ_000.ASC*) containing the desired random numbers will be created. The default name of the related protocol file is *ZZ_000.CON*.

In conclusion you will obtain the following new files for the complete generation procedure (if you always use the default file names):

ZZ_000.BIN - Binary random bit file
ZZ_000.LOG - Protocol file concerning *ZZ_000.BIN*
ZZ_000.ASC - ASCII random number file
ZZ_000.CON - Protocol file concerning *ZZ_000.ASC*

Trouble Shooting

If you get repeated error messages:

- Check existence of following USB driver files in your Windows directories

`c:\windows\inf\ezusbw2k.inf`
`c:\windows\system32\drivers\ezusb.sys`

(The directory "c:\windows\inf\" may be hidden in the Windows Explorer.)

If you don't find the files copy them from the directory ...*ZRANDOM-USB-Driver*\ on the ZRANDOM CD ROM to your Windows directories.

- Disconnect and reconnect the USB connector. Then, restart generation.
- Avoid usage of task manager or other programs during random bit generation.
- It may be necessary to rename *ezusb.sys* to *CyUsb.sys*, and then to overwrite the already existing file `c:\windows\system32\drivers\CyUsb.sys`

Terms and conditions of trade / Liability

Claims for damage, non-functionality and mis-shipping must be made within seven days of receipt. Customers are responsible for ensuring safe delivery of the returned item. The warranty expires if the devices have been opened.

We are not liable for damages which result from an inappropriate use of our products. Limitations on usage: Our products should only be used for civilian applications.

Technical modifications remain reserved.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL WESTPHAL ELECTRONIC BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES HOWEVER CAUSED (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, LOSS OF BUSINESS INFORMATION, BUSINESS INTERRUPTION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR THE INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WESTPHAL ELECTRONIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Technical Specifications

ZRANDOM USB external device:

- Input current: max. 100 mA (supplied by USB connector)
- Maximum internal voltage: + 5 V
- Cable connection: Standard USB
- Working temperature range: 0 °C ... +40 °C
- Storage temperature range: -10 °C ... +70 °C
- Dimensions: 175 mm x 113 mm x 36 mm
- Weight: 305 g

WESTPHAL ELECTRONIC
Kritzegraben 6
07743 Jena
Germany
FAX: ++ 49 3641 228802
info@westphal-electronic.com
www.westphal-electronic.com
www.westphal-electronic.de
