Introduction to libQRNG library

Jarosław A. Miszczak
Institute of Theoretical and Applied Informatics, Polish Academy of Sciences
Baltycka 5, 44-100 Gliwice, Poland

07/05/2012 (v. 0.02)

Note: Functions provided by libQRNG are described in libQRNG.h header file.

1 Establishing the connection with the QRGN server

In order to retrieve data from the QRNG service provided by the PicoQuant and the Department of Physics of Humboldt University, it is necessary to register on the service web page [1]. In order to establish a connection with the server one can use one of the functions

- qrng_connect(qrng_username, qrng_password) – establish a connection with the QRNG service (qrng.physik.hu-berlin.de:4499),
- qrng_connect_SSL(qrng_username, qrng_password) – establish a secure connection with the QRNG service using SSL.

Both functions require a username and a password provided during the registration. The connection is closed using qrng_disconnect() function.

- qrng_disconnect() – close the connection with the QRNG server.

2 Retrieving random data

QRNG service allows to retrieve random data in the form of integer numbers, double precision numbers or bytes. Integer and double precision numbers can be retrieved in form of single values or arrays, while bytes can be retrieved only in arrays.

2.1 Base functions

The following two functions allow to retrieve single numbers of type **int** or **double**:

- **int** qrng_get_int(**int** *val) – get single **int** and put at val,
- **int** qrng_get_double(**double** *val) – get single **double** and put at val.

2.2 Functions for operating on arrays

The following functions allow to retrieve arrays of numbers of type **int** or **double**.

- **int** qrng_get_int_array(**int** *arr, **int** dim, **int** *ac) – get dim integer numbers and put them into arr array

- **int** qrng_get_double_array(**double** *arr, **int** dim, **int** *ac) – get dim double precision numbers and put them into arr array

The above functions report the actual number of retrieved numbers and put this information in ac.

References

[1] QRNG Service, http://qrng.physik.hu-berlin.de

[2] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, *An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements*, Appl. Phys. Lett. 98, 171105 (2011) http://dx.doi.org/10.1063/1.3578456