PROCEEDINGS OF SCIENCE

Quality testing of data from photon-based hardware random number generator

Dmitriy Beznosko [a,*], Keith Driscoll [b], Fernando Guadarrama [c], Alexander Iakovlev [d], Steven Mai [c] and Nikolas Thornton [c]

a College of STEM, School of Sciences, Clayton State University,
2000 Clayton State Blvd, Morrow, GA 30260 USA,

b College of STEM, Department of Mathematics, Clayton State University,
2000 Clayton State Blvd, Morrow, GA 30260 USA

c College of STEM, CSIT Department, Clayton State University,
2000 Clayton State Blvd, Morrow, GA 30260 USA

d Upper School Science Department, Woodward Academy,
1662 Rugby Avenue, College Park, GA 30337

E-mail: dmitriybeznosko@clayton.edi

Hardware random number generators (HRNG) are widely used in the computer world for security purposes as well as in the science world as a source of the high-quality randomness for the models and simulations. Currently existing HRNG are either costly or very slow and of questionable quality. This work proposes a simple design of the HRNG based on the low-number photon absorption by a detector (a photo-multiplier tube of a silicon-based one i.e. SiPM, MPPC, etc.) that can provide a large volume of high-quality random numbers. The prototype design, different options of processing and the testing of quality of the generator output are presented.

42nd International Conference on High Energy Physics (ICHEP2024)
18-24 July 2024
Prague, Czech Republic

[*] Speaker

PoS(ICHEP2024)1215

1. Introduction

The most widespread random number generator that is used for most of the applications is pseudo-random number generators, or PRNGs. The truly random numbers without this need of the initial seed can be generated using a hardware random number generator (HRNG).

A way to avoid external influence is to use quantum-level effects, for example, by using photon detectors that are generally based on quantum-level principles and thus are not susceptible to the minute changes in environment. With that, high quality random numbers can be generated [1]. Two separate approaches to photon detection are presented, one with a photo-multiplier tube (PMT) and the other one using a Hamamatsu [2] multi-pixel photon counter (MPPC). The quality of the output of each approach is discussed.

2.Experimental Setup Description

The following two setups were used: PMT and MPPC-based. The PMT setup included a Hamamatsu H11284-30 PMT in a black box, The source of light was the light emitting diode (LED). The PMT was biased at 1750 V and read by the CAEN [3] DT5730 Flash Analog-to-Digital Converter (FADC). The components for this setup were provided by the DUCK [4 ,5] collaboration, their system design is described in more detail in [6, 7].

The second setup uses the output from the 1.3x1.3 mm2 MPPC that is connected to the ADC on the Arduino Nano board that also controls the attached LED and the Hamamatsu C11204-01 power supply. The Arduino communicates the amplitudes via serial data (via USB) to the data acquisition PC. Further information on the hardware details is available in [8].

3. Data Analysis

The amplitude data is collected from both setups. This data requires further processing to generate a random bitstream. Two methods of processing have been implemented.

The *first* processing method is that of High/Low. If amplitude is higher than previous, then it adds a 1 to the bitstream. If it is lower, then it adds a 0. This flawed approach was used to generate low-quality data for comparison purposes. The *second* (good) method is the Even/Odd. For every amplitude, if it is even (all amplitudes are integers), then 1 is added to the bitstream. If the value is odd, then 0 is added. Von Neumann's procedure is used to clean all the datasets from possible deviations from 50/50 of 1s and 0s [8]. This is done to illustrate if the dataset has a vital flaw or can be improved or fixed.

4. Testing Methods

For this work, 3 tests have been selected and implemented for determining the quality of output from both processing methods applied to each HRNG setup data. These tests are as follows: the Arithmetic Mean and Standard Deviation (AMSD) test, the Monte Carlo Pi Estimation (MCPE) test, and the Fractional Line Symmetry (FLS) test [8, 9].

5.Data Quality Analysis

For the analysis, the data sample of the same size was chosen for each setup (290 000 bits). The 'bad' data resulting from high-low processing is used to show the sensitivity of each test.

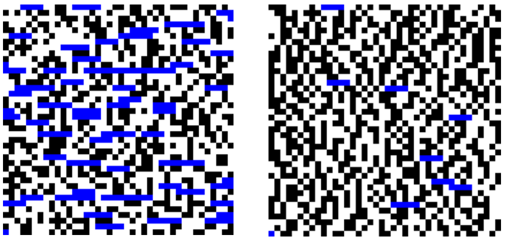
From Table 1, the AMSD test is not sensitive to the 'bad' data. The MCPE test is more sensitive. Note that the MPPC operating parameters were not optimized for this test and do influence the data quality somewhat. For the FLS test, the following parameters were used: detect length of 4, estimated line count for 290,000 bits is 11328. The FLS test results (Table 2) are very sensitive to the flaw in the 'bad' data by showing the asymmetry between the horizontal and vertical lines. Graphically, this is shown in Figure 1. The application of the Von Neumann's procedure doesn't fully fix the 'bad' data. No significant difference in data quality between the setups is observed.

Table 1: The results of the AMSD and MCPE tests for both setups.

PMT SETUP		**MPPC SETUP**	
Even/Odd	*High/Low ('bad data')*	*Even/Odd*	*High/Low ('bad data')*
Monte Carlo Pi Estimation:			
Pre-Neumann: 3.13644	Pre-Neumann: 3.45441	Pre-Neumann: 3.08083	Pre-Neumann: 3.47953
Post-Neumann: 3.14502	Post-Neumann: 3.09256	Post-Neumann: 3.11290	Post-Neumann: 3.07141
Average:			
Pre-Neumann: 0.49946	Pre-Neumann: 0.49992	Pre-Neumann: 0.50791	Pre-Neumann: 0.49971
Post-Neumann: 0.49947	Post-Neumann: 0.49872	Post-Neumann: 0.50059	Post-Neumann: 0.50052
Standard Deviation:			
Pre-Neumann: 0.499999711	Pre-Neumann: 0.499999994	Pre-Neumann: 0.499937370	Pre-Neumann: 0.499999913
Post-Neumann: 0.499999723	Post-Neumann: 0.499998371	Post-Neumann: 0.499999653	Post-Neumann: 0.499999734

Table 2: The results of the FLS test for both setups.

PMT SETUP		**MPPC SETUP**	
Even/Odd	*High/Low ('bad data')*	*Even/Odd*	*High/Low ('bad data')*
Horizontal lines:			
Pre-Neumann: 11337.5	Pre-Neumann: 2042.25	Pre-Neumann: 10647.5	Pre-Neumann: 1415.0
Post-Neumann: 10990.0	Post-Neumann: 11981.25	Post-Neumann: 11004.75	Post-Neumann: 11143.75
Vertical lines:			
Pre-Neumann: 11291.75	Pre-Neumann: 11359.75	Pre-Neumann: 10545.75	Pre-Neumann: 10563.5
Post-Neumann: 11006.25	Post-Neumann: 10495.25	Post-Neumann: 11002.5	Post-Neumann: 9683.25



(a) (b)

Figure 1. High/low pre-Neumann PMT horizontal lines for: (a) - Even/Odd, (b) – High/Low data.

To demonstrate the overall high quality of the MPPC setup data, all tests were run on the large data sample with the results in Table 3.

Table 3: The results of all tests for large data sample from the MPPC setup.

Test:	Pre-Neumann	Post-Neumann
Bitstream length	4 080 132	4 034 062
Average	0.4946018903309991	0.49971517542367966
Stdev	0.4999708595628366	0.4999999188749541
Value of Pi:	3.14531246079	3.14534395228
FLS lines estimate:	*159380*	*157580*
Vertical lines	165238.25	157620.75
Horizontal lines	165015.0	158293.25

Table 3 shows that the data from MPPC setup is of high quality, and that using the Von Neumann's procedure marginally improved the data quality, mostly notable in the FLS test results.

6. Conclusion and Future Plans

The photon-based solutions explored in this research have shown great potential for being high-speed sources of high-quality random number generation. The best way to process data is the even/odd method. The PMT appears to outperform the MPPC in the MCPE Test, but the MPPC setup is still in its prototype stage and needs tuning of the runtime parameters.

By use of the FLS Test, it was detected that the high/low method of processing is far worse than the even/odd method as expected. The FLS Test successfully revealed this despite the high/low algorithm output passing the other tests relatively well.

Current objectives for the future of this project are to sync the MPPC Arduino with an LED that is voltage controlled through DAC. A proper enclosure for the board and sensor is also necessary, as well as a faster board to increase the number of amplitudes per second.

Acknowledgements

This work was supported in part by NSF LEAPS-MPS Award 2316097 and by Clayton State University College of Arts & Sciences UCARE grant, FY 2023-24.

References

[1] D. Beznosko et al., *Random Number Hardware Generator Using Geiger-Mode Avalanche Photo Detector*, PoS(PhotoDet2015)049, DOI: 10.22323/1.252.0049,

[2] HAMAMATSU PHOTONICS K.K., Electron Tube Division, 314-5, Shimokanzo, Iwata City, Shizuoka Pref., 438-0193, Japan

[3] CAEN S.p.A. Via della Vetraia, 11, 55049 Viareggio Lucca, Italy

[4] Beznosko, D.; Aseykin, V.; Dyshkant, A.; Iakovlev, A.; Krivosheev, O.; Krivosheev, T.; Shiltsev, V.; Zhukov, V. Prototype Setup Hardware Choice for the DUCK System. *Quantum Beam Sci.* **2024**, *8*, 17. https://doi.org/10.3390/qubs8030017

[5] Dmitriy Beznosko, Valeriy Aseykin, Alexander Dyshkant, Alexander Iakovlev, Oleg Krivosheev, Tatiana Krivosheev, Valeriy Zhukov, *DUCK Detector System Design*, PoS(ICRC2023)187. DOI: https://doi.org/10.22323/1.444.0187

[6] Dmitriy Beznosko, Valeriy Aseykin, Shriya Chakraborti, Alexander Dyshkant, Gerald Harris, Alexander Iakovlev, Oleg Krivosheev, Tatiana Krivosheev, Nicholas Muong, Alexander Ramirez, Vladimir Shiltsev, and Valeriy Zhukov. *Prototype Setup for the DUCK*, Proceedings of *3rd Annual College of STEM Symposium*, PROC(03ACSS2024)003, 05/2025, https://sos.clayton.edu/proceedings/003/PROC(03ACSS2024)003.pdf

[7] Dmitriy Beznosko, Valeriy Aseykin, Alexander Dyshkant, Alexander Iakovlev, Oleg Krivosheev, Tatiana Krivosheev, Valeriy Zhukov, *Design Considerations of the DUCK Detector System*, *Quantum Beam Sci.* **2023**, 7(1), 6; https://doi.org/10.3390/qubs7010006

[8] Dmitriy Beznosko, Keith Driscoll, Fernando Guadarrama, Steven Mai, Nikolas Thornton, *Data Analysis Methods Preliminaries for a Photon-based Hardware Random Number Generator*, arXiv:2404.09395, 2024/4/15, https://doi.org/10.48550/arXiv.2404.09395

[9] Dmitriy Beznosko, Keith Driscoll, Fernando Guadarrama, Steven Mai, and Nikolas Thornton. "Preliminaries of a Photon-based Hardware Random Number Generator Design and Data Analysis Methods", Proceedings of *3rd Annual College of STEM Symposium*, PROC(03ACSS2024)001, 05/2025, https://sos.clayton.edu/proceedings/003/PROC(03ACSS2024)001.pdf