Analysis of the effects of temperature increase on quantum random number generator

Yuanhao Li, Yangyang Fei, Weilong Wang, Xiangdong Meng, Hong Wang, Qianheng Duan and Zhi Ma

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, China
Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, Henan, 450001, China

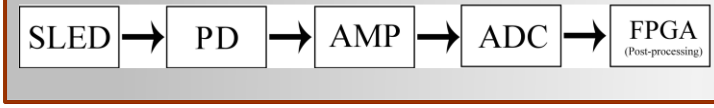
Introduction

Quantum random number generator (QRNG) relies on the intrinsic randomness of quantum mechanics to produce true random numbers which are important in many fields.

QRNGs with semiconductor light source have attracted a lot of attention due to their operational simplicity and high generation rate. However, the temperature of light source may vary due to imperfect devices and other factors. There is still a lack of study on the effects of temperature variations on the security of practical QRNG.

We fill this gap by presenting a numerical method for studying the effects of temperature increase on the super-luminescent emitting diode (SLED) based QRNG and propose some strategies toward robust QRNG against temperature increase.

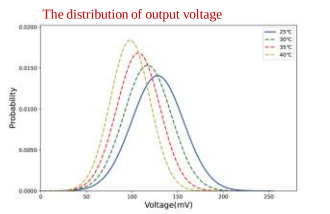
SLED based QRNG



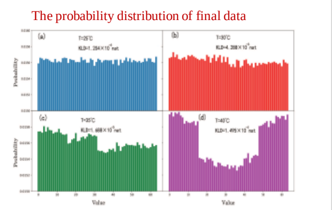
SLED → PD → AMP → ADC → FPGA (Post-processing)

QRNG consists of the SLED, the photon detector (PD), the amplifier (AMP), the analog-to-digital converter (ADC) and the field programmable gate array (FPGA)

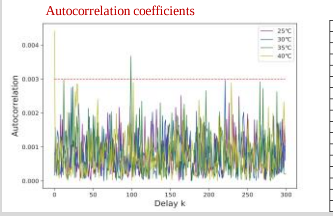
Randomness analysis of output sequence with temperature increase



The distribution of output voltage



The probability distribution of final data



Autocorrelation coefficients

NIST Statistical Test

Test	25°C	30°C	35°C	40°C
Frequency	Pass	Pass	Failure	Pass
BlockFrequency	Pass	Pass	Pass	Pass
CumulativeSums	Pass	Pass	Failure	Pass
Runs	Pass	Pass	Pass	Failure
LongestRun	Pass	Pass	Pass	Pass
Rank	Pass	Pass	Pass	Pass
FFT	Pass	Pass	Pass	Pass
NonOverlappingTemplate	Pass	Pass	Pass	Failure
OverlappingTemplate	Pass	Pass	Pass	Pass
Universal	Pass	Pass	Pass	Pass
ApproximateEntropy	Pass	Pass	Pass	Pass
RandomExcursions	Pass	Pass	Pass	Pass
RandomExcursionsVariant	Pass	Pass	Pass	Pass
Serial	Pass	Pass	Failure	Pass
LinearComplexity	Pass	Pass	Pass	Pass
Result	Success	Success	Failure	Failure

The output voltage of SLED-based QRNG fits with Gaussian distribution. The increase of temperature leads to the decrease of mean value and standard deviation of the output voltage, where the ratio of mean value and the standard deviation of the output voltages at different temperatures is constant.[1]

In our simulation experimental, the minimum entropy of the raw data is 6.15 and the post-processing algorithm is XOR operation and 6-LSB method at 25℃. With the increase of temperature, the distribution of the output voltage is changed, but the parameters of ADC and post-processing method to process raw data are the same at different temperatures.

The KLD value becomes larger as the temperature increases, which means a big difference between the probability distribution of final data and the uniform distribution. Moreover, some values of autocorrelation coefficients are larger than $3\sigma_a$=0.003 and the final data cannot pass the NIST Statistical Test at 35 ℃ and 40℃. This is because the mean value and the standard deviation of the light intensity decrease as the temperature of semiconductor diode increases, which leads to the min-entropy lower than 6. The raw data are still processed by the same XOR operation and 6-LSB method, which extracts too many bits from the raw data.

Strategies toward robust QRNG against temperature increase

The robust post-processing methods are complex post-processing method[2], Toeplitz hashing randomness extractor[3] and MLP method[4]. The raw data processed by these robust post-processing methods can all pass the NIST randomness test at different temperatures from 25℃ to 40℃.

Besides, the min-entropy decreases with the increase of temperature. According to the results of numerical simulation, the min-entropy is smaller than 6 when the temperatures of SLED are 35℃ and 40℃. resulting in that the min-entropy is overestimated. By real-time monitoring the min-entropy of output sequence from the QRNG, security of the QRNG can be guaranteed. Moreover, monitoring the temperature variations of SLED is also a straight and effective method.

NIST Statistical Test

Test	Complex post-processing[2]				Toeplitz hashing[3]				MLP[4]			
	25°C	30°C	35°C	40°C	25°C	30°C	35°C	40°C	25°C	30°C	35°C	40°C
Frequency	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
BlockFrequency	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
CumulativeSums	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Runs	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
LongestRun	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Rank	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
FFT	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
NonOverlappingTemplate	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
OverlappingTemplate	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Universal	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
ApproximateEntropy	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
RandomExcursions	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
RandomExcursionsVariant	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Serial	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
LinearComplexity	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Result	Success	Success	Success	Success	Success	Success	Success	Success	Success	Success	Success	Success

[1] C.R.S. Williams, J.C. Salevan, X. Li, R. Roy, T.E, *Opt. Express* **18**, 23584–23597 (2010).
[2] Y. Liu, M.-Y. Zhu, B. Luo, J.-W. Zhang, H. Guo, *Laser Phys. Lett.* **10**, 045001 (2013)
[3] X. Ma et al., *Phys. Rev. A* **87**, 062327 (2013)
[4] D.A. Karras, V. Zorkadis, *International Joint Conference on Neural Networks* (2003)

This paper has been published on European Physical Journal D.
DOI: 10.1140/epjd/s10053-021-00087-7