Random Quantum Noise Generation Using Shot Noise In Semiconductors

Jakub Niemczuk*

Wroclaw University of Science and Technology
jakubniemczuk@gmail.com

Abstract

This paper describes the proposal of a fully electronic quantum noise source for random number generators used in mathematics and quantum cryptography. It uses the phenomena of shot noise generated by current carriers in reverse polarized semiconductor junctions due to quantum tunneling. This device is built to present that the shot noise in simple semiconductor devices can be amplified and sampled, to produce a random bits data stream.

This is the first iteration.

Introduction

Random number generators are used to generate random data for many applications like mathematics, statistics, physical simulation and encryption. There are two types of random number generators, true- and pseudo-random number generators. The second type generates randomness by calculating numbers with an algorithm. Its output can be predicted by knowing the algorithm behavior and/or the seed of the generator. True random number generators produce randomness from unpredictable physical phenomena, like for example weather fluctuations[1] or phase fluctuations of lasers[2]. In the group of true random generators there are devices that use quantum uncertainty for very high entropy generation. Unpredictable quantum effects are used, for example the choice of photons passing through a light beamsplitting optical path[3]. But those devices, even when they perform well, are not cheap, simple and miniature enough to be implemented in every communication device or computer station. This paper describes the first attempt in building a quantum true random number generator that draws its entropy from shot noise in semiconductors. Using shot noise as a source of quantum entropy allows to build a true random number generator without costly and bulky optics, expensive lasers or photodetectors.

*Faculty of Microsystem Electronics and Photonics

1. Noise in semiconductors

In all electrical devices we can observe the presence of noise. In semiconductor devices noise is created via a number of different physical phenomena. For example in a semiconductor diode the known noise components are: [8]

- Thermal Noise,
- Shot Noise,
- Generation-Recombination Noise,
- $1/f$ Noise,
- $1/f^2$ Noise,
- Burst Noise/RTS Noise,
- Avalanche Noise.

1.1. Thermal Noise

Thermal noise or Johnson-Nyquist noise is created due the random motion of carriers in every conducting device caused by thermal excitation. The noise spectral density is white and constant over a very wide spectrum. RMS voltage and current value is given by:

$$v_n = \sqrt{4kTR\Delta f} \tag{1}$$

$$i_n = \sqrt{\frac{4kT\Delta f}{R}} \tag{2}$$

where:

k is Boltzmann's constant in joules per kelvin,
T is the absolute temperature in kelvins,
R is the device resistance in ohms,

Δf is the frequency range of the noise taken into account.

1.2. Shot Noise

Shot Noise comes from the discrete structure of electrical current. It is created by current fluctuations during current flow via a p-n junction barrier. It is temperature independent and, like the Thermal Noise, white in a wide frequency spectrum. RMS value of the fluctuating current is given by:

$$i_n = \sqrt{2qI\Delta f} \tag{3}$$

where:

q is the elementary charge of an electron,
I is the current flowing through the device.

Shot noise is mostly observed in semiconductor devices, such as p-n junctions, tunnel junctions and other. Its presence can be even observed in metallic resistors[4].

1.3. Generation-Recombination Noise

Generation-recombination noise results from fluctuations in the number of current carriers in semiconductors. Those fluctuations leads to dynamic changes in conductance of the device. The spectral density of this type of noise if given by:

$$\frac{S(f)}{N^2} = \frac{(\overline{\Delta N})^2}{N^2} \cdot \frac{4\tau}{1 + (2\pi f\tau)^2} \tag{4}$$

where:

$\overline{\Delta N})^2$ is the variance in carriers N,
τ is the carrier lifetime,
f is the frequency.

This noise is constant to a certain frequency of $f = 1/(2\pi\tau)$, and after that it is decreasing proportionally like $1/f^2$ noise.

1.4. $1/f$ and $1/f^2$ noise

$1/f$ noise, often called flicker noise, is the dominant noise component at lower frequencies with a spectral density proportional to $1/f$. The two major models of $1/f$ noise are:

- Model developed by McWhorter[5],
- Model developed by Hooge[6].

The $1/f^2$ noise is observed in metallic connections in electronic circuits. The spectral density of those two noises can be approximated by:

$$S(f) \propto \frac{\beta}{f^\alpha} \tag{5}$$

where α and β are constants.

1.5. Burst Noise/RTS Noise

Burst noise also called 'popcorn noise' is a type of noise that resembles square impulses of fixed amplitude and random duration and appearance. This type of noise is temperature, current, voltage and even semiconductor mechanical stress dependent. But using Machlups model we can describe the spectral density of this noise as[7]:

$$S(f) = \frac{C}{f_w[1 + (\frac{f}{f_w})^2]} \tag{6}$$

where:

$$C = \frac{abc^2}{\pi(a+b)^2} \tag{7}$$

$$f_w = \frac{a+b}{2\pi} \tag{8}$$

a, b, c are constants that depend on the type and even specimen of the semiconductor.

The spectral density of this type of noise is flat till frequency f_w, after which it is decreasing proportional to to $1/f$.

1.6. Avalanche Noise

Avalanche noise results from from avalanche current multiplication in reverse biased p-n junctions. It occurs at an avalanche breakdown when carriers gain enough energy to create another electron-hole pair in collisions with the crystal lattice. This is a random process. The spectral density of this noise is given by:

$$S(f) = \frac{2qI}{(2\pi f\tau)^2} \tag{9}$$

where I is the average value of the reverse biasing current.

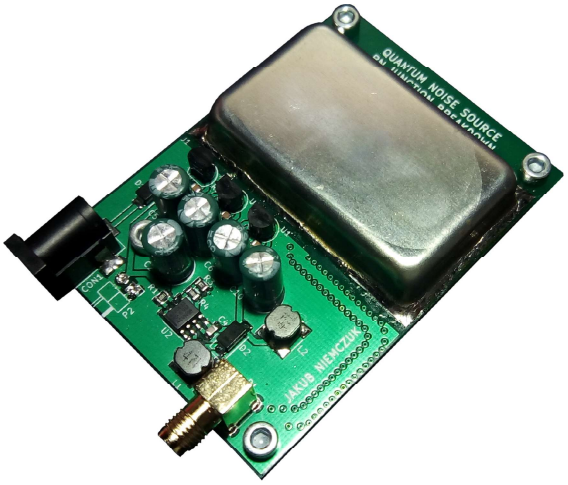

Figure 1: *A photograph of the physics package that generates raw random bitstream.*

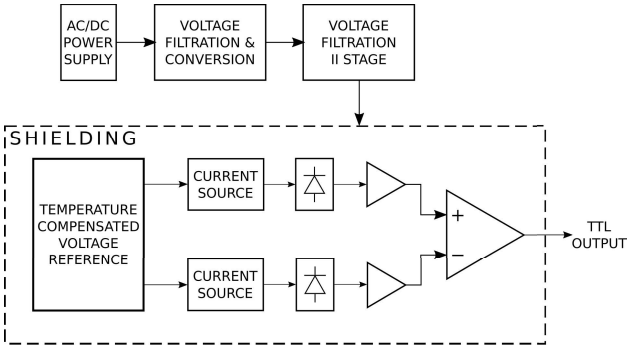

Figure 2: *Block diagram of the device.*

2. First Device Proposal

This device is the first attempt in creating a hardware random number generator. It was partially inspired by Charles Platt and Aaron Logue work[9]. But it was improved and rearranged. Namely the power supply section is significantly complicated to eliminate any external power supply noise coupling. The most sensitive part of the circuit is shielded by a ferromagnetic steel cap to eliminate any electromagnetic interference. Not one but two, thermally coupled, noise sourcing semiconductor devices are used, from which the noise signals are compared together, to eliminate thermal drift.

Fig.2 shows the block diagram of the device. It consists of two major blocks. First block is responsible for voltage conversion and filtration to eliminate the influence of external noise. The second block is a shielded cavity with an additional voltage reference that drives two current sources, that together with current mirrors apply constant current to two reverse polarized diode junctions. The current sources are pushing approximately 10 μA through reverse polarized pn junctions inside two npn bipolar transistor. The base-emitter junction are dropping about 5 V. The two noise signals generated via reverse current, flowing through junctions, are amplified and then compared between each other. Using this technique together with matched components and thermal coupling, the impact of the temperature drift was reduced. The comparator outputs a TTL compatible bit stream. Fig.3 shows amplified signal from one of the noise sources and Fig.4 shows the distribution of noise samples that resembles Poisson distribution.

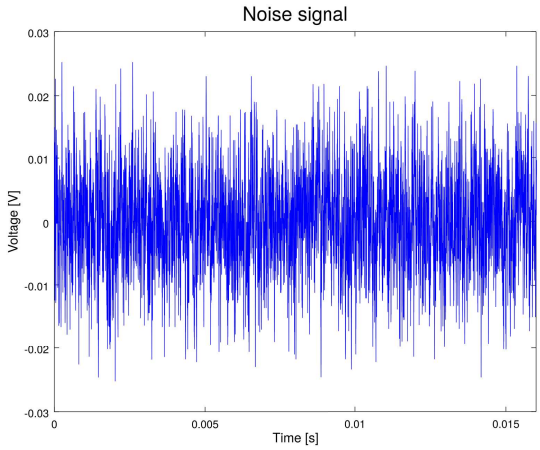

Figure 3: *Sample of the amplified shot noise. Sample interval 400 ns.*

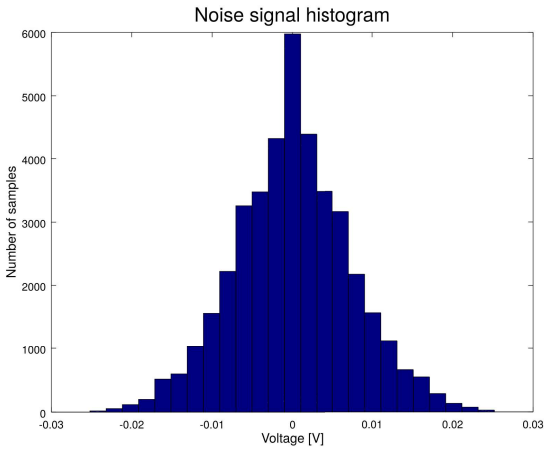

Figure 4: *Histogram of the noise sample captured by oscilloscope.*

3. Data Capturing and Analysis

The data was captured with a constant sample rate via an Atmel AVR microcontroller and send through serial to a PC. Fig.5 shows the TTL waveform sampled by the microcontroller. For bias removal the method presented by John von Neumann was used[9]. A histogram of a random picked block of numbers (after the bias removal) the size of 100000 uint8 values is presented in Fig.6. Fig.7 shows a 512 x 512 pixels bitmap, created from a random picked small raw data sample, where are no patterns visible. For randomness testing the software package "DieHarder" was used. The "DieHarder" package consists of series of tests suitable for testing random number generators[10]. If the data generated from this setup was truly random it would pass most of the tests. Unfortunately a large sample passed only first three major tests and failed the rest with some exceptions, that could be false positives.

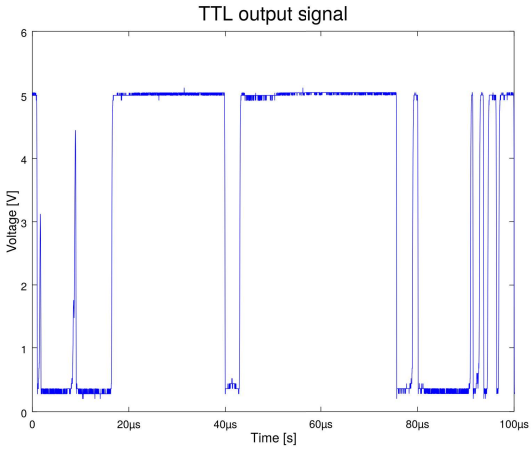

Figure 5: *Sample of the TTL output signal.*

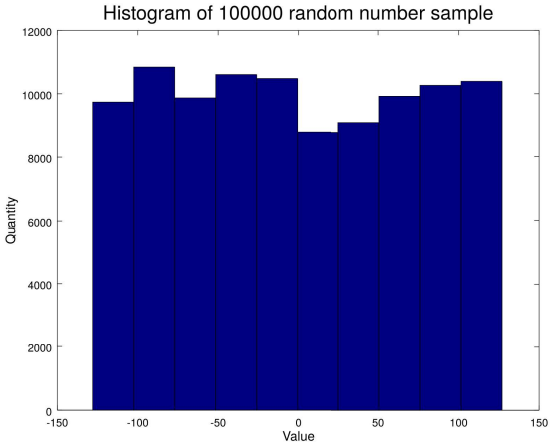

Figure 6: *Histogram of a random picked block of numbers the size of 100000 uint8 values.*

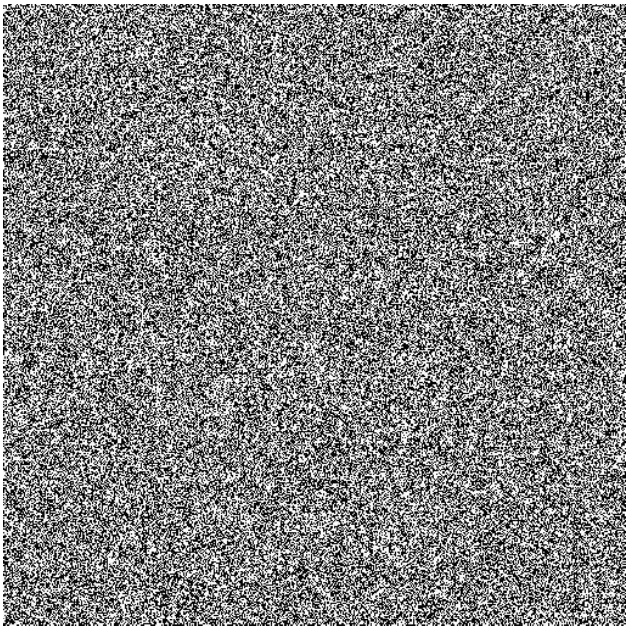

Figure 7: *512 x 512 bitmap created from a small raw sample.*

4. Discussion

The small uneven distribution of numbers together with a slightly bias, even after applying the von Neumann method, can be present probably due the $1/f$ noise taking a significant part in long time data sampling. The bigger the sample, the bigger the irregularity of the frequency spectrum generated bu this version of the device. In the second iteration care of pink noise should be taken. Also for a truly **quantum** random number generator thermal noise should be eliminated whose origin comes from classical physics. Instead trying to stabilize the bias and amplitude of the signal generated on a reverse polarized pn junction, to satisfy von Neumanns method, more effort should be put into other debiasing methods, that don't relay on the time stability of the data input. For example methods proposed by Boaz Barak, Ronen Shaltiel and Eran Tromer[11].

```
$ dieharder -a -g 201 -f random0_tmpcpy1.bin
#=============================================================================#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown          #
#=============================================================================#
   rng_name    |           filename             |rands/second|
 file_input_raw|             random0_tmpcpy1.bin|  3.11e+07  |
#=============================================================================#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#=============================================================================#
   diehard_birthdays|   0|       100|     100|0.82076730|  PASSED
      diehard_operm5|   0|   1000000|     100|0.50891570|  PASSED
  diehard_rank_32x32|   0|     40000|     100|0.67785857|  PASSED
```

Figure 8: *The report for the first three "DieHard" tests on a collected sample.*

References

[1] Dr Mads Haahr. Random number generator website that generates randomness via atmospheric noise. `https://www.random.org/`

[2] Jie Yang, Jinlu Liu, Qi Su, Zhengyu Li, Fan Fan, Bingje Xu, Hong Guo. *5.4 Gbps real time quantum random number generator with simple implementation*, Optics Express 27275, 2016, Vol. 24, No. 24.

[3] Andre Stefaonv, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard and Hugo Zbinden. *Optical quantum random number generator*, Journal of Modern Optics, 2000, 47:4, pp. 595-598, DOI:10.1080/09500340008233380.

[4] Marc de Jong *Sub-Poissonian shot noise*, Published in Physics World, August 1996, page 22.

[5] McWhorter A. L. *1/f noise and germanium surface prosperities. In Semiconductor Surface Physics.* R. H. Kingdton (Ed.), University of Pennsylvania Press, Philadelphia, PA, 1957, pp. 207âĂŞ228.

[6] Hooge F. N. *1/f noise is no surface effect. Physics Letters*, 29A (3), 1969, 139-140.

[7] Lech Hasse, Ludwik Spiralski, *Szumy elementów i układów elektronicznych*, Wydawnictwo Naukowo-Techniczne, 1981, pp. 92-95.

[8] Alicja Konczakowska, B. M. Wilamowski. *Noise in Semiconductor Devices - Industrial Electronics Handbook*, vol. 1 Fundamentals of Industrial Electronics, 2nd Edition, chapter 11, pp. 11-1 to 11-12, CRC Press 2011.

[9] Charles Platt, Aaron Logue. *Really, Really Random Number Generator*, Make: Projects, Make Magazine, 2016. `https://makezine.com/projects/really-really-random-number-generator/`

[10] Robert G. Brown, Dirk Eddelbuettel, David Bauer. *Dieharder: A Random Number Test Suite*, Duke University Physics Department, Durham. `https://webhome.phy.duke.edu/~rgb/General/dieharder.php`

[11] Boaz Barak, Ronen Shaltiel, Eran Tromer. *True Random Number Generators Secure in a Changing Environment*, In Workshop on Cryptographic Hardware and Embedded Systems (CHES), of LNCS, pp. 166-180, 2003.