Q-RAND: Random number generation from quantum confinement semiconductors

Thomas McGrath
Physics Department
Lancaster University
Lancaster, UK
contact@tpmcgrath.co.uk

Abstract*—Q-RAND presents a means of producing physically-derived random numbers that are indeterminate at the quantum level, through a process derived from the quantum confinement of a resonant tunnelling diode. This system presents many advantages for the production of these random numbers - including the macroscopically measurable nature of the diode's resultant behavior, which allows for the use of non-specialized support electronics and hardware prototype design. Random number generators of this type are especially valuable for cybersecurity applications, and this phase of the Q-RAND project seeks to produce and refine a hardware design to provide high bandwidth randomness through the operation of a miniature standalone device.

I. Background

Randomly generated numbers, or sources of randomness in general, are valuable for a range of applications, from cryptography to statistics and even gaming. Many contemporary random number generators rely on algorithmic pseudo-randomness [1], where the stream of numbers are algorithmically derived from a prior explicit digital state. These techniques rely on the obfuscation of the internal state or the algorithm itself for any unpredictability, and while fast and easy to implement exposure to the evolving internal state of the generator presents vulnerability for cryptographic purposes.

A solution to this are devices called true random number generators, which derive randomness from the physical world [2]. These typically operate by interfacing with the messy non-digital environment directly, such as sampling using an analogue to digital converter or examining the free-running oscillation for rings of inverter gates [3], [4]. The highest standard of unpredictability for true random number generators are those that derive their randomness from quantum systems [5]. To the surprise of physicists in the early 20th century, it has been found that there are elements to a physical system on the quantum level that are not only hard to capture state information for, but for which it is fundamentally impossible to do so [6], [7]. These quantum-level indeterminate systems can be exploited to produce fundamentally unpredictable randomness, and it is through quantum confinement semiconductors that we aim to do this here.

The semiconductor devices we use in this work are known as the resonant tunnelling diodes, or RTDs [8]. These diodes consist of two conduction band barriers defining a quantum well, for which electrons can either tunnel through (if their energy aligns with an intermediate confined energy level), or with enough energy bypass (over the barrier structure entirely), through a process known as thermionic emission [9].

This paper presents the current prototype for the standalone version of this evaluation system, with emphasis on the electronics surrounding (and performing the evaluations of) the RTD. The aim of this device is to extract randomness from the RTD and relay to a host via USB connection, with an amount of processing and system control occurring on-chip.

II. Related Work

Quantum random number generators (QRNGs) of various forms have already been developed. The first QRNGs derived their randomness from the physical process of nuclear decay [10]. These devices typically derived random bits from the time intervals between measured particle decays in the nuclei of a collection of atoms. While it is easy to see that this system is quantum indeterminate it requires specialised measurement equipment, usually a Geiger–Müller tube, and typically requires the use of radioactive sources to increase the count rate enough to allow for a reasonable throughput.

More recently, quantum random numbers are produced via evaluating quantum optical effects [11], most recognisably through measuring the path of single photons through a half-silvered mirror (requiring single photon emitter/detectors) [12], laser evaluation of quantum vacuum state fluctuations [13], or through shot noise taken from conventional charge-coupled device photodetectors [14]. As these techniques all require conversion from the optical domain to the electronic, there has been work done to develop all-electronic QRNGs, in particular through specific sources of noise in electronic circuits. This noise is typically that which emerges from single-barrier quantum tunnelling events, such as that from a reversed bias Zener diode [15]. In contrast to double-barrier tunnelling, in these devices there is no confined energy level to provide transmission at a single electronic voltage/energy level to the exclusion of others, meaning the physical consequences of each quantum event are much less distinct, requiring precise amplification, measurement and general consideration for the separation of quantum events from thermal noise.

III. Current Prototype

The Q-RAND device extracts random numbers from the RTD by pulsing the diode with electrical current of deliberate amplitude and duration such that it is possible, indeterminate and in the ideal case equiprobable for the electrons to either tunnel through the double barrier structure or to bypass the diode through thermionic emission (Figure 1a) [16]. From an macroscopic electronic perspective these two transmission modes mean the RTD exhibits negative differential resistance, and an N shaped IV characteristic [17]. Using a current source one can imagine pulsing electrons at the current value of the peak of this N shape (defined by electron tunnelling) such that it is not possible to tell whether the voltage measured across the device will remain at the voltage level of this peak or at the voltage projection on the second positive differential resistance region beyond (Figure 1b). This can also be achieved in the voltage domain with a well-chosen load resistor, such that the voltage distribution between this resistor and the RTD is bistable in the same way.

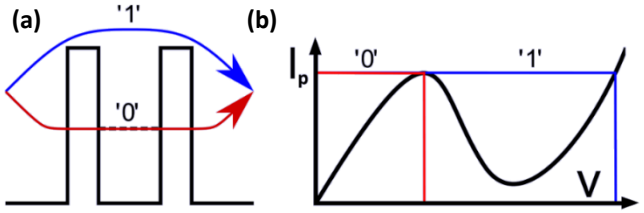

Figure 1: A diagram to show the principle of operation for the RTD based RNG. (a) The band structure of the RTD showing the two transmission modes. (b) The IV characteristic of the RTD, showing the two current pulsing outcomes.

The current prototype for the USB Q-RAND consists of three parts - the microcontroller board, the interconnect daughterboard and the RTD chip and carrier. The microcontroller used in this project was the SAMD21G18 from Microchip Technology. This was chosen due to the relatively high clock speed, allowing for higher throughput and temporal resolution, and for the 10-bit on-chip digital to analogue converter to allow adjustments of voltage pulse amplitude directly without any further components. This microcontroller was provided alongside supporting components on the Seeed studio 'XIAO SAMD21' development board (Figure 2a, 2b), and connected to the interconnect daughterboard through the use of header pins.

The daughterboard connects the microcontroller to the RTD unit, with additional components to enhance and enable the operation of the system (Figure 2c). These include voltage-limiting diodes to avoid overloading the RTD and a load resistor. This board also contains two 2N7002H n-channel MOSFETs - one in series and one to ground as a means of pulsing voltage, alongside a TLV3501 high speed comparator. In the current firmware version these aren't used in lieu of on-chip microcontroller functional equivalents.

The final part of the system relates to the RTD itself. The RTDs were grown in III/V material via microwave beam epitaxy [18], with the wafer diced with a diamond scribe, secured to 28-pin chip carriers with epoxy resin and bonded to chip pins with a wire bonder. These chips were then inserted into a plastic leaded chip carrier sockets bonded to the daughterboard (Figure 2b), with a grounded conductive polylactic acid cover 3D printed and placed over the top to protect against duct, contact and electromagnetic interference (Figure 2a). To select one RTD within each chip a wire is hand-soldered to through holes on the edge of the daughterboard connecting the broken out chip carrier pins to their circuit input and output in the desired configuration.

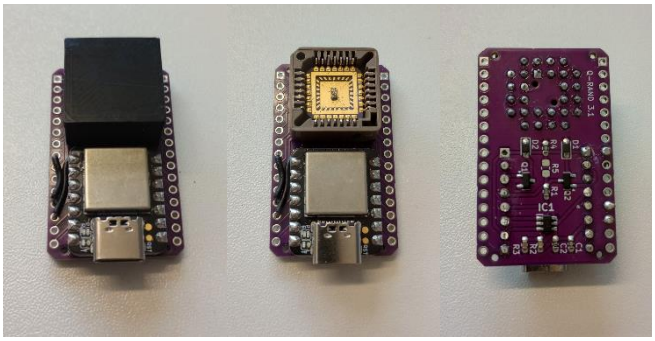

Figure 2: Photographs of the current Q-RAND prototype. (a) The top side of the device, with RTD shield. (b) The font side of the device with RTD shield removed. (c) The back side of the device.

The first design of the microcontroller firmware was written in C++ with a heavy reliance on Arduino libraries made compatible with the microcontroller in question, with these being phased out to direct register manipulation as RNG throughput (and thus operational speed) is optimised. Communication between the prototype and the host device occurs over USB via a virtual COM port. This port is read by a packaged python executable running on the host device which performs further postprocessing and saves the random output to disk based on user parameters.

IV. Future Work

Relating to hardware, in future revisions it is hoped to transition to a more minimal electronic design, taking forward only what is most conducive to random number generation. In addition, further steps can be taken to maximise the throughput of the random number generator. A previous iteration of this design was experimented with using a Complex Programable Logic Device (CPLDs) circuit for enhanced post-processing throughput, defined using the hardware definition language VHDL, and the use of a Field Programable Gate Array (FPGA) integrated circuit may be optimal for control and processing going forward. Additionally, a more encompassing enclosure would be desirable for client handling.

Going forward, it would also be desirable for the firmware controlling the microcontroller to be written entirely in an lower level embedded language without the use of Arduino libraries, while including more complex control logic and health tests - both for testing the hardware, as well as the validity of random bit stream. Finally, relating to software it would be desirable to have a driver such that the device can interact with the host operating system at a lower level, allowing the device to add to the internal entropy pool directly. Once the prototype design is optimised, it is hoped to proceed to a stage of industry-standardised testing and certification, followed by small order manufacture.

V. Responsible innovation

Enhancing the cryptographic systems that we rely on as foundational to modern life, whether local to a user or on a wider scale, can be considered a pro-social application of technology. Additionally, the employment of non-cryptographic randomness is a vital tool for research in the name of further positive causes - from statistical sampling to Monte Carlo simulation.

Ensuring minimal power consumption (and the resultant environmental impact) is also a consideration for this project - the current prototype and resonant tunnel diode design dissipates a few nanojoules per bit (further reducible by adjusting semiconductor fabrication specifications), with the peripheral electronics designed such to to capitalise on this. The power for this device is provided by the USB of the host device with the hope of renewable upstream power, and any future portability or host-less RNG beacon functionality intended to use rechargeable, sustainable power banks.

The current prototype of the Q-RAND uses a conductive polylactide faraday shield and protective cover. These were fabricated through the low-waste technique of fused deposition, using a material that is recyclable and industrially compostable.

VI. Author bio

The author of this work is researcher in the physics of the topic discussed herein, with an interest in electronic device prototyping both for the realisation of this system and for projects more generally.

VII. Acknowledgments

The author would like to thank Professor Robert Young and Dr Ramon Bernardo Gavito for their guidance and foundational work on this project. This work is part of the development occurring at Quantum Base Ltd, a quantum security company based out of Lancaster University bringing scientific discovery to commercial application.

VIII. References

[1] E. B. Barker, W. C. Barker, W. E. Burr, W. T. Polk, and M. E. Smid, 'Recommendation for key management, part 1 : general (revision 3)', National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-57p1r3, 2012. doi: 10.6028/NIST.SP.800-57p1r3.

[2] Ç. K. Koç, Ed., *Cryptographic engineering*. New York, NY, USA: Springer, 2009.

[3] S. N. Dhanuskodi, A. Vijayakumar, and S. Kundu, 'A Chaotic Ring oscillator based Random Number Generator', in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Arlington, VA: IEEE, May 2014, pp. 160–165. doi: 10.1109/HST.2014.6855588.

[4] A. T. Markettos and S. W. Moore, 'The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators', in *Cryptographic Hardware and Embedded Systems - CHES 2009*, vol. 5747, C. Clavier and K. Gaj, Eds., in Lecture Notes in Computer Science, vol. 5747. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 317–331. doi: 10.1007/978-3-642-04138-9_23.

[5] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, 'Quantum random number generation', *npj Quantum Inf*, vol. 2, no. 1, p. 16021, Jun. 2016, doi: 10.1038/npjqi.2016.21.

[6] W. Heisenberg, 'Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik', *Zeitschrift fur Physik*, vol. 43, pp. 172–198, Mar. 1927, doi: 10.1007/BF01397280.

[7] H. P. Robertson, 'The Uncertainty Principle', *Phys. Rev.*, vol. 34, no. 1, pp. 163–164, Jul. 1929, doi: 10.1103/PhysRev.34.163.

[8] L. L. Chang, L. Esaki, and R. Tsu, 'Resonant tunneling in semiconductor double barriers', *Applied Physics Letters*, vol. 24, no. 12, pp. 593–595, 1974, doi: 10.1063/1.1655067.

[9] B. Ricco and M. Ya. Azbel, 'Physics of resonant tunneling. The one-dimensional double-barrier case', *Phys. Rev. B*, vol. 29, no. 4, pp. 1970–1981, Feb. 1984, doi: 10.1103/PhysRevB.29.1970.

[10] S. Takeuchi and T. Nagai, 'Random pulser based on photon counting', *Nuclear Instruments and Methods in Physics Research*, vol. 215, no. 1–2, pp. 199–202, Sep. 1983, doi: 10.1016/0167-5087(83)91309-1.

[11] M. Herrero-Collantes and J. C. Garcia-Escartin, 'Quantum random number generators', *Rev. Mod. Phys.*, vol. 89, no. 1, p. 015004, Feb. 2017, doi: 10.1103/RevModPhys.89.015004.

[12] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, 'A fast and compact quantum random number generator', *Review of Scientific Instruments*, vol. 71, no. 4, pp. 1675–1680, Apr. 2000, doi: 10.1063/1.1150518.

[13] C. Gabriel *et al.*, 'A generator for unique quantum random numbers based on vacuum states', *Nature Photon*, vol. 4, no. 10, pp. 711–715, Oct. 2010, doi: 10.1038/nphoton.2010.197.

[14] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, 'Quantum Random Number Generation on a Mobile Phone', *Phys. Rev. X*, vol. 4, no. 3, p. 031056, Sep. 2014, doi: 10.1103/PhysRevX.4.031056.

[15] P. I. Somlo, 'Zener-diode noise generators', *Electron. Lett.*, vol. 11, no. 14, p. 290, 1975, doi: 10.1049/el:19750219.

[16] R. Bernardo-Gavito *et al.*, 'Extracting random numbers from quantum tunnelling through a single diode', *Sci Rep*, vol. 7, no. 1, p. 17879, Dec. 2017, doi: 10.1038/s41598-017-18161-9.

[17] Jian Ping Sun, G. I. Haddad, P. Mazumder, and J. N. Schulman, 'Resonant tunneling diodes: models and properties', *Proceedings of the IEEE*, vol. 86, no. 4, pp. 641–660, Apr. 1998, doi: 10.1109/5.663541.

[18] M. Md Zawawi, K. Ian, J. Sexton, and M. Missous, 'Fabrication of Submicrometer InGaAs/AlAs Resonant Tunneling Diode Using a Trilayer Soft Reflow Technique With Excellent Scalability', *Electron Devices, IEEE Transactions on*, vol. 61, pp. 2338–2342, Jul. 2014, doi: 10.1109/TED.2014.2322107.