SCIENTIFIC REP⚙RTS

OPEN

Extracting random numbers from quantum tunnelling through a single diode

Ramón Bernardo-Gavito[1], Ibrahim Ethem Bagci[2], Jonathan Roberts[1], James Sexton[3], Benjamin Astbury[1], Hamzah Shokeir[1], Thomas McGrath[1], Yasir J. Noori[1], Christopher S. Woodhead[1], Mohamed Missous[3], Utz Roedig[2] & Robert J. Young[1]

Random number generation is crucial in many aspects of everyday life, as online security and privacy depend ultimately on the quality of random numbers. Many current implementations are based on pseudo-random number generators, but information security requires true random numbers for sensitive applications like key generation in banking, defence or even social media. True random number generators are systems whose outputs cannot be determined, even if their internal structure and response history are known. Sources of quantum noise are thus ideal for this application due to their intrinsic uncertainty. In this work, we propose using resonant tunnelling diodes as practical true random number generators based on a quantum mechanical effect. The output of the proposed devices can be directly used as a random stream of bits or can be further distilled using randomness extraction algorithms, depending on the application.

Random number generators (RNGs) are important in diverse applications such as cryptography, simulations, testing, address generation, and gaming[1]. Many current implementations rely on pseudo-random number generators, but information security requires true random numbers for sensitive applications like key generation in banking, defence or even social media. True random number generators are systems whose outputs cannot be determined, even if their internal structure and response history are known[1]. It has been demonstrated that true random numbers can be obtained from different sources such as noise[2], chaotic systems[3] and quantum phenomena[4]. The main advantage of using sources of quantum noise is its intrinsic uncertainty, as opposed to the predictability of classical sources of noise. In this work, we propose using quantum tunnelling in a simple semiconductor structure, namely a resonant tunnelling diode (RTD). These devices are practical and scalable sources of randomness whose behaviour is governed by quantum physics at room temperature. The semiconductor nature of RTD's, and the simple system proposed to read random numbers from them, makes them a promising candidate for integration into microelectronic systems. The potential to integrate single elements RNGs into current technologies makes them resistant to frequency injection and biasing attacks, which affect state-of-the-art RNGs such as those based on free running oscillators[5]. The output of these devices can be directly used as a random stream of bits or can be further distilled using randomness extraction algorithms, depending on the application.

Resonant tunnelling diodes are the technological realisation of a semiconductor quantum well (QW) with finite rectangular barriers[6,7]. They consist of a thin, narrow band-gap semiconductor structure acting as a quantum well between two wide band-gap semiconductor tunnelling barriers[8,9]. Beyond the tunnelling barriers, highly doped regions of the narrow band-gap semiconductor are usually referred to as the emitter/collector regions, analogous to those in traditional bipolar transistors. Recently, resonant tunnelling devices using quantum dots[10,11], atomic-scale defects[12], graphene[13,14] and other two-dimensional materials[15,16] have been demonstrated, and this has renewed the interest in investigating resonant tunnelling and its applications using new materials. A high-resolution image of a typical RTD used in this work[8], consisting of a square mesa (containing the quantum well structure) and an air bridge (for electrical connection), can be seen in Fig. 1a.

When swept with a DC voltage source, RTDs show the characteristic N-shaped I-V curve of negative differential resistance devices. A typical RTD characteristic is shown in Fig. 1b. The current obtained on the first slope of

[1]Physics Department, Lancaster University, Lancaster, LA1 4YB, UK. [2]School of Computing and Communications, Lancaster University, Lancaster, LA1 4WA, UK. [3]School of Electrical and Electronic Engineering, University of Manchester, Manchester, M13 9PL, UK. Correspondence and requests for materials should be addressed to R.J.Y. (email: r.j.young@lancaster.ac.uk)
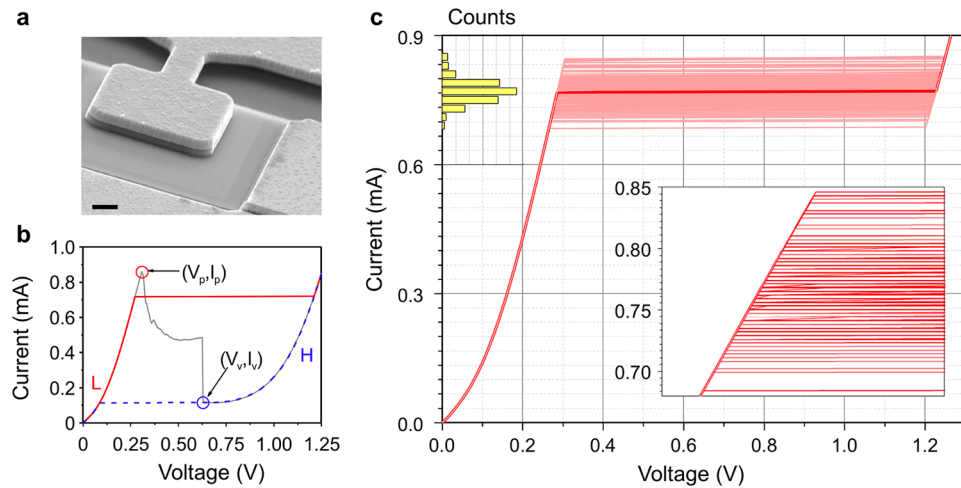
1

Figure 1. Physical and electrical characteristics of RTDs. (**a**) SEM micrograph of one of the studied 25 μm^2 RTDs taken with a tilt of 20 degrees (scale bar 1 μm). (**b**) I-V characteristic of a 4 μm^2 RTD showing the NDR curve with a voltage sweep (grey line) and the hysteretic behaviour with current sweeps. A jump from the low-resistance state to the high-resistance state can be observed in forward sweeps (red line) near the peak, and the opposite will happen in reverse sweeps (blue line) near the valley. (**c**) 100 forward current sweeps (light red lines) showing the random distribution of state changes around an average value (bold red line). This average curve corresponds to the red line shown in (**b**). The histogram shows the switching probability as a function of current (same vertical units as the main axis). The inset shows a zoom-in to the switching region.

the curve arises due to the resonant tunnelling process[6,17] that gives this device its name. Here, the bias voltage has shifted the first QW state between the emitter's Fermi level and the lower edge of its conduction band, facilitating the resonant tunnelling of electrons and allowing a reasonably high current to be measured. Once the confined level falls below the conduction band, a sudden drop in current can be observed, as there are no more occupied states in the emitter aligned with the QW state. Further increase of the voltage leads to an increase in the current due to other conduction processes such as thermionic emission of hot electrons over the two tunnelling barriers[17]. The sudden current drop occurring between the two conduction regimes appears as a narrow resonance in the I-V characteristics. The bistability[18] and fast switching characteristics[19] emerging from the sharp NDR resonance of RTDs make them promising candidates for applications in multi-valued logic circuits[20], random-access memories[21], multi-function logic gates[22], chaotic signal generation[3,23,24], single-photon switching[25], unique device identification[26] and terahertz oscillators[27,28].

Due to their N-shaped NDR characteristics, the RTD's current is a single-valued function of voltage whereas the opposite is not true, as current values between those of the peak (I_p) and the valley (I_v) exhibit multiple voltage levels[18] due to the different conduction mechanisms. Using a current source in that range can result in two different scenarios: a low-resistance state (L) corresponding to the first positive differential resistance (PDR) region, and a high-resistance state (H) corresponding to the second PDR region. The instability of the NDR region[29,30] prevents the system from staying in that voltage range for long times, pushing the system to one of the two PDR branches. Ramping the current up and down results in a hysteresis cycle[31,32] between these two resistance states as shown in Fig. 1b.

For the experiments carried on in this work we used a set of RTDs fabricated as described elsewhere[8]. In particular the chips we used contain hundreds of RTDs of different sizes (4, 9, 16, and 25 μm^2), whose current-voltage characteristics scale with size, with minor differences between individual devices due to the fabrication process[26], i.e. the current density-voltage characteristics are similar for all the device sizes. In the text only the results for 4 μm^2 and 9 μm^2 devices are shown for the sake of brevity.

Results and Discussion

Figure 1 shows that sweeping current across the device results in a hysteresis cycle. The forward sweep takes place in the first PDR region up to a threshold near the peak current where the voltage is pushed to the second PDR region of the curve. Once that threshold is passed, ramping down the current will not push the voltage back to the first PDR region until the valley current is reached. Our measurements show that the switching threshold from one state to the other is not a fixed value but is statistically distributed near the resonance current, I_p (Fig. 1c). As expected, currents above I_p will always send the system to the second PDR region as the low-resistance branch does not reach that current range, and setting the current below I_v will always give the low resistance state for similar reasons. On the other hand, working between I_v and I_p results in a non-deterministic switching behaviour, as the state change from one slope to the other happens at different values each time following a probability distribution as shown in the histogram of Fig. 1c. The origin of the uncertainty on the response of the RTD to current sources is most likely related to the charge build-up and trap filling in the quantum well and adjoining regions. This leads to shifts in the energy of the confined level[6,18], dynamically altering the threshold at which resonant tunnelling occurs.
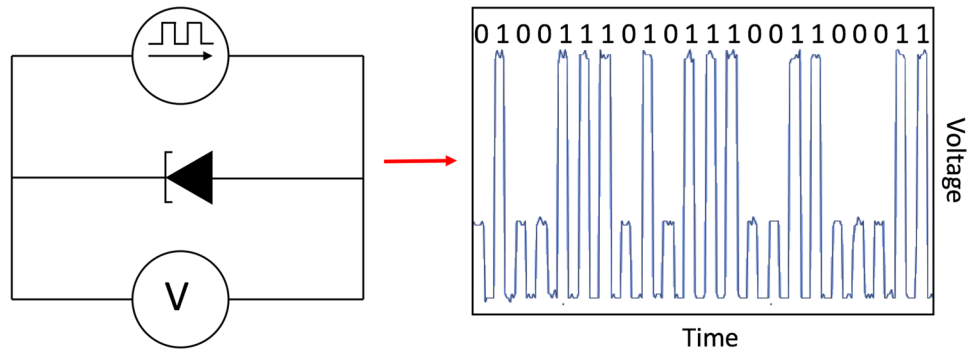
Figure 2. The experimental arrangement used to generate random numbers. A pulsed current source drives the RTD while the voltage across it is measured. The right panel shows an oscilloscope trace illustrating the random response, along with the corresponding logical levels.
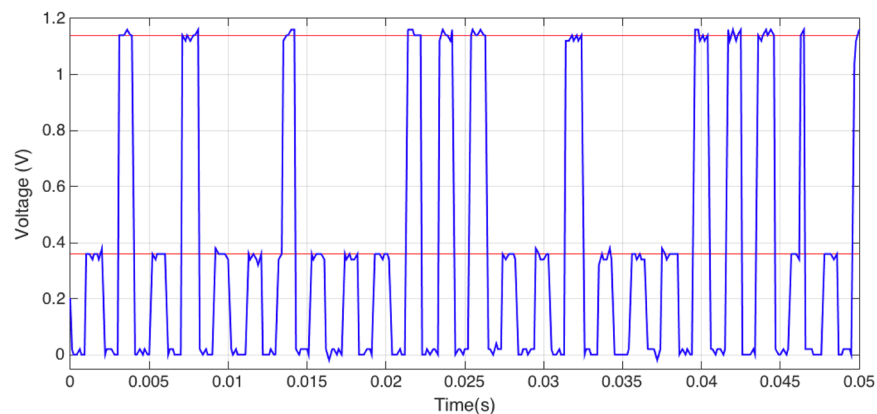

Figure 3. Time dependent voltage measurements of a 9 μm² RTD driven with a pulse train of 1.50 mA, 1 ms pulse width, 50% duty cycle. The red lines mark the position of the LOW and HIGH levels. The voltage pulses measured at 13 ms and 46 ms show the transition from LOW to HIGH during the corresponding current pulse.

To further characterise this stochastic switching behaviour and exploit its possibilities as an eventual random number generator, we performed a series of experiments using current pulse trains of varying amplitude and frequency. A Keithley 2602B source-measure unit (SMU) is programmed to send periodic current pulses of a fixed amplitude and length. For the sake of simplicity and keeping a small parameter space, the duty cycle of the pulse trains is kept at 50%, while varying the amplitude and pulse width. The voltage drop across the RTD is measured with the SMU at the end of each pulse, resulting in a value either in the first or second PDR regions. Alternatively, the output voltage can be measured using a fast oscilloscope to characterise the time response of the system. A schematic of the experimental setup is shown in Fig. 2.

Analysing the time response of different RTDs to current pulse trains shows that the random behaviour of the switching threshold is a dynamic process. This relates to the time that it takes the system to jump between the first and second PDR regions. When the source is set at a fixed current, the device will start conducting in the first PDR region of the I-V curve, i.e. that dominated by resonant tunnelling through the first quantum well state, and after a period of time it will jump into the second PDR region. A typical example of this behaviour can be seen in Fig. 3, with some pulses staying at the low state, some jumping straight to the high state and a few of them undergoing the jump during the pulse.

This dynamic switching behaviour can be related to the charge accumulation in the quantum well or in charge traps distributed along the structure, which are known to have an influence in the behaviour of RTDs[6,18]. The charge and discharge of these features lead to a shift in the energy of the confined quantum level, thus allowing switching from one tunnelling mechanism to another. The quantum nature of the randomness generation of this system emerges from the charge accumulation in the quantum well and charge traps, which is known to be a dynamic process that can take from picoseconds to hundreds of milliseconds[6], which fits well with our experimental results.

In order to operate RTDs as sources of randomness, we can exploit the aforementioned random dynamic switching to obtain a stream of random bits. By sourcing current pulses to an RTD and measuring the voltage drop across the device at a given time, i.e. at the end of each pulse, we will obtain a value that corresponds either to the first or second PDR regions. To simplify the description of the operation we will denote these two states as
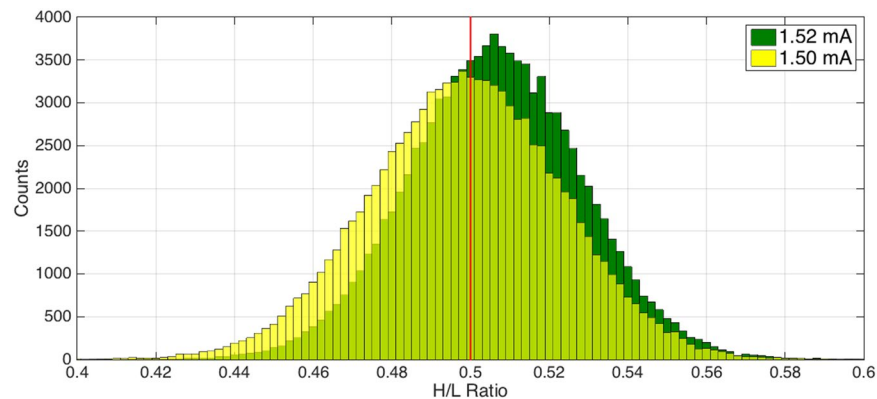
3

Figure 4. High to low ratio tuning as a function of pulse amplitude. The high to low ratio of the RTD can be tuned by changing the current amplitude of the pulses. The graph shows two histograms of the output distribution of two different pulse trains, 1ms wide, 50% duty cycle with different current amplitudes, namely 1.50 mA (yellow) and 1.53 mA (dark green). The red line marks the 50/50 point. The results show how we can tune the average output of a RTD-based RNG by changing the current level. Each histogram corresponds to a sample size of 5×10^7 pulses divided in subsets of 500 pulses.

L and H respectively. The experiment shows that the the L/H ratio depends both on the current level and the pulse width, which allows us to easily change the probability distribution of the output, as shown in Fig. 4.

Considering the dynamic behaviour described above, the output will be a random distribution of L and H values with characteristics depending upon the amplitude and width of the pulses. For low currents and short pulses the distribution will be strongly biased towards L, while high currents and long times will make the output more likely to be H. Tuning these two parameters allows us to set the probability distribution of the output. This can be explained by considering that the charge trapping, which is responsible for the switching between the two conduction mechanisms, is a probabilistic effect itself. A higher current corresponds to a larger number of electrons crossing the device in a given time, so more charge can be trapped, assuming a fixed probability. Likewise, if the pulse is longer, it is more probable that at the end of the pulse the trapped charge is enough to push the confined level to higher energies and facilitate the alternative conduction path.

Most applications employing random numbers, such as cryptography, require an unbiased uniform output distribution. In other cases, shifted or skewed distributions might be required. For example, a shifted probability distribution can be useful for simulating the random path of a particle subject to a certain potential, or they may be used in gambling or stock market predictions. One potential advantage of an RTD-based random number generator is that its average output can be modified *in operando*, which can be exploited for more complex simulations.

Our experiments show that, although the underlying principle of operation of the RTD as an RNG is the quantum tunnelling through the resonant structure, it is convoluted with classical thermal noise and other types of noises from the measurement equipment. Variations in the environment temperature and electrical noise can influence the output of the proposed RNG. Our experiments show a slow drift correlated to the evolution of the room temperature. Although this effect can be considered to add up to the randomness itself, as it will push the L/H ratio out of the set point in a random way, it is undesirable for most applications. Also, it adds a strong source of classical noise to a device that is intended to be used as a quantum random number generator. The use of a simple feedback mechanism to correct for temperature swings mitigates the effect of thermal drift, as it is a very slow process compared to pulse period. Regardless, the operating principle discussed still involves a classical measurement of a quantum process, making the system subject to any classical sources of noise that can obfuscate the pure quantum randomness.

The problem of discriminating between classical and quantum randomness sources has already been addressed in previous work, and there exist randomness extraction algorithms specifically designed to distil the output from quantum RNGs to obtain uniformly distributed random numbers. As an example, we used the double-hash function algorithm suggested by Frauchiger et al.[33], which is computationally efficient and could be implemented in hardware. The resulting data successfully passes the 15 tests in the NIST randomness test suite[34] with a significance level of 0.05 (5%). Specific details on testing are given in the supplementary information.

Conclusion

In this paper, we have shown how the uncertainty in the switching between two conduction mechanisms in a resonant tunnelling diode can be exploited to produce a random number generator. This uncertainty emerges from the charge accumulation process in the quantum well and surrounding traps states. These charges alter the energy landscape for the incoming electrons, eventually impeding them to undergo a resonant tunnelling process and forcing them to conduct exclusively via thermionic emission.

The operating voltages of the two conduction states can be easily mapped to digital logic to generate a random bit stream. Although the raw output of the proposed scheme is still affected by classical noise, it can be used for many applications requiring random numbers. Distilling the raw output using a double-hash function to correct

the effect of the classic environment results in bit streams that complies with the NIST suite of randomness tests, a standard in random number generator testing for cryptographic applications.

Although the random bit generation speed shown in our experiment is low compared to state-of-the-art random number generators, this is due to the particular choice of our experimental setup. The charge trapping process to which we attribute the random switching behaviour can take place in the range of picoseconds to hundreds of milliseconds, so in principle nothing prevents using faster pulsed sources up to even GHz. Thus, we consider that it is physically possible to increase the bit rate by several orders of magnitude, but the steps required to do that require further engineering research that is beyond the scope of this proof of concept paper.

One of the advantages of RTDs used in this study is that the operating voltage levels can be easily interfaced with logic levels in microelectronics. In the example above, the first PDR region lays below 0.4 V, i.e. before the resonance. At the working currents this means that the L level will be close to this voltage. The corresponding H level for that current projected to the second PDR region corresponds to around 1.15 V.

References

1. Koç, Ç. K. & Stipcevic, M. In *Open Problems in Mathematics and Computational Science* (ed Çetin Kaya Koç) 275-316 (Springer, 2014).
2. Marangon, D. G., Vallone, G. & Villoresi, P. Random Bits, True and Unbiased, from Atmospheric Turbulence. *Sci Rep* **4**, 5490, https://doi.org/10.1038/srep05490 (2014).
3. Maezawa, K., Kawano, Y., Ohno, Y., Kishimoto, S. & Mizutani, T. Direct Observation of High-Frequency Chaos Signals from the Resonant Tunneling Chaos Generator. *Japanese Journal of Applied Physics* **43**, 5235–5238, https://doi.org/10.1143/jjap.43.5235 (2004).
4. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum Random Number Generation. *npj Quantum Information* **2**, 16021, https://doi.org/10.1038/npjqi.2016.21 (2016).
5. Markettos, A. T. & Moore, S. W. The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators. *Cryptographic Hardware and Embedded Systems - Ches 2009, Proceedings* **5747**, 317–331 (2009).
6. Ricco, B. & Azbel, M. Y. Physics of Resonant Tunneling. *The One-Dimensional Double-Barrier Case. Physical Review B* **29**, 1970–1981, https://doi.org/10.1103/PhysRevB.29.1970 (1984).
7. Chang, L. L., Esaki, L. & Tsu, R. Resonant Tunneling in Semiconductor Double Barriers. *Applied Physics Letters* **24**, 593–595 (1974).
8. Zawawi, M. A. M., Ian, K. W., Sexton, J. & Missous, M. Fabrication of Submicrometer InGaAs/AlAs Resonant Tunneling Diode Using a Trilayer Soft Reflow Technique With Excellent Scalability. *Ieee T Electron Dev* **61**, 2338–2342, https://doi.org/10.1109/Ted.2014.2322107 (2014).
9. Paul, D. J. *et al*. Si/Sige Electron Resonant Tunneling Diodes with Graded Spacer Wells. *Applied Physics Letters* **78**, 4184, https://doi.org/10.1063/1.1381042 (2001).
10. Chen, G., Klimeck, G., Datta, S., Chen, G. & Goddard, W. A. Resonant Tunneling Through Quantum-Dot Arrays. *Physical Review B* **50**, 8035–8038, https://doi.org/10.1103/PhysRevB.50.8035 (1994).
11. Lee, K. W. *et al*. Light-Induced Negative Differential Resistance in Graphene/Si-Quantum-Dot Tunneling Diodes. *Sci Rep* **6**, 30669, https://doi.org/10.1038/srep30669 (2016).
12. Di Paola, D. M. *et al*. Resonant Zener Tunnelling Via Zero-Dimensional States in a Narrow Gap Diode. *Sci Rep* **6**, 32039, https://doi.org/10.1038/srep32039 (2016).
13. Britnell, L. *et al*. Resonant Tunnelling and Negative Differential Conductance in Graphene Transistors. *Nat Commun* **4**, 1794, https://doi.org/10.1038/ncomms2817 (2013).
14. Mishchenko, A. *et al*. Twist-Controlled Resonant Tunnelling in Graphene/Boron Nitride/Graphene Heterostructures. *Nat Nanotechnol* **9**, 808–813, https://doi.org/10.1038/nnano.2014.187 (2014).
15. Nguyen, L. N. *et al*. Resonant Tunneling Through Discrete Quantum States in Stacked Atomic-Layered Mos2. *Nano Lett* **14**, 2381–2386, https://doi.org/10.1021/nl404790n (2014).
16. Guerrero-Becerra, K. A., Tomadin, A. & Polini, M. Resonant Tunneling and the Quasiparticle Lifetime in Graphene/Boron Nitride/Graphene Heterostructures. *Physical Review B* **93**, https://doi.org/10.1103/PhysRevB.93.125417 (2016).
17. Sze, S. M. & Ng, K. K. *Physics of Semiconductor Devices*. 3 edn, 415-465 (John Wiley & Sons, Inc., 2006).
18. Sheard, F. W. & Toombs, G. A. Space-Charge Buildup and Bistability in Resonant-Tunneling Double-Barrier Structures. *Applied Physics Letters* **52**, 1228–1230, https://doi.org/10.1063/1.99165 (1988).
19. Kluksdahl, N. C., Kriman, A. M., Ferry, D. K. & Ringhofer, C. Transient Switching Behavior of the Resonant-Tunneling Diode. *Ieee Electr Device L* **9**, 457–459, https://doi.org/10.1109/55.6944 (1988).
20. Yan, Z. X. & Deen, M. J. A New Resonant-Tunnel Diode-Based Multivalued Memory Circuit Using a Mesfet Depletion Load. *Ieee J Solid-St Circ* **27**, 1198–1202, https://doi.org/10.1109/4.148329 (1992).
21. Ternent, G. & Paul, D. J. Si/SiGe Tunneling Static Random Access Memories. *ECS Transactions* **50**, 987–990, https://doi.org/10.1149/05009.0987ecst (2013).
22. Chen, K. J., Akeyoshi, T. & Maezawa, K. Monostable Bistable Transition Logic Elements (Mobiles) Based on Monolithic Integration of Resonant-Tunneling Diodes and Fets. *Jpn J Appl Phys* **1**(34), 1199–1203, https://doi.org/10.1143/Jjap.34.1199 (1995).
23. Kawano, Y., Kishimoto, S., Maezawa, K. & Mizutani, T. Resonant Tunneling Chaos Generator for High-Speed/Low-Power Frequency Divider. *Jpn J Appl Phys* **2**(38), L1321–L1322, https://doi.org/10.1143/Jjap.38.L1321 (1999).
24. Kawano, Y., Kishimoto, S., Maezawa, K. & Mizutani, T. Robust Operation of a Novel Frequency Divider Using Resonant Tunneling Chaos Circuit. *Japanese Journal of Applied Physics Part 1-Regular Papers Short Notes & Review Papers* **39**, 3334–3338, https://doi.org/10.1143/Jjap.39.3334 (2000).
25. Weng, Q. *et al*. Quantum Dot Single-Photon Switches of Resonant Tunneling Current for Discriminating-Photon-Number Detection. *Sci Rep* **5**, 9389, https://doi.org/10.1038/srep09389 (2015).
26. Roberts, J. *et al*. Using Quantum Confinement to Uniquely Identify Devices. *Sci Rep* **5**, 16456, https://doi.org/10.1038/srep16456 (2015).
27. Orihashi, N., Hattori, S., Suzuki, S. & Asada, M. Experimental and Theoretical Characteristics of Sub-Terahertz and Terahertz Oscillations of Resonant Tunneling Diodes Integrated with Slot Antennas. *Japanese Journal of Applied Physics* **44**, 7809–7815, https://doi.org/10.1143/jjap.44.7809 (2005).
28. Asada, M. & Suzuki, S. Theoretical Analysis of External Feedback Effect on Oscillation Characteristics of Resonant-Tunneling-Diode Terahertz Oscillators. *Japanese Journal of Applied Physics* **54**, 070309, https://doi.org/10.7567/jjap.54.070309 (2015).
29. Kidner, C., Mehdi, I., East, J. R. & Haddad, G. I. Power and Stability Limitations of Resonant Tunneling Diodes. *Ieee T Microw Theory* **38**, 864–872, https://doi.org/10.1109/22.55778 (1990).
30. Kidner, C., Mehdi, I., East, J. R. & Haddad, G. I. Bias Circuit Instabilities and their Effect on the Dc Current Voltage Characteristics of Double-Barrier Resonant Tunneling Diodes. *Solid State Electron* **34**, 149–156, https://doi.org/10.1016/0038-1101(91)90081-9 (1991).

31. Savel'ev, S. E., Marchesoni, F. & Bratkovsky, A. M. Mesoscopic Resistive Switch: Non-Volatility, Hysteresis and Negative Differential Resistance. *The European Physical Journal B* **86**, https://doi.org/10.1140/epjb/e2013-40966-4 (2013).
32. Strukov, D. B., Snider, G. S., Stewart, D. R. & Williams, R. S. The Missing Memristor Found. *Nature* **453**, 80–83, https://doi.org/10.1038/nature06932 (2008).
33. Frauchiger, D., Renner, R. & Troyer, M. True Randomness from Realistic Quantum Devices. *Preprint at* https://arxiv.org/abs/1311.4547 (2013).
34. Lawrence E. Bassham, I. *et al.* SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. (National Institute of Standards & Technology, 2010).

Author Contributions

R.J.Y., U.R. and R.B.-G. designed the project. M.M. and J.S. fabricated and performed initial tests on the RTD devices. R.B.-G., J.R., C.S.W., B.A. and H.S. performed the detailed electronic measurements. R.B.-G., I.E.B., T.M. and Y.J.N. analysed the data. The manuscript was prepared primarily by R.B.-G., and R.J.Y. with contribution from all authors.

Additional Information

Supplementary information accompanies this paper at https://doi.org/10.1038/s41598-017-18161-9.

Competing Interests: The authors declare that they have no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.