Atomic-scale Authentication Using Resonant Tunnelling Diodes

J. Roberts[1], I. E. Bagci[2], M. A. M. Zawawi[3], J. Sexton[3], N. Hulbert[1], Y. J. Noori[1], M. P. Young[1], C. S. Woodhead[1], M. Missous[3], M. A. Migliorato[3], U. Roedig[2] and R. J. Young[1]

The rapid development of technology has unintentionally provided a wealth of resources that has enabled the trust of everyday interactions to be undermined[1]. Authentication schemes aim to address this challenge by providing proof of identity. This can be achieved by using devices that, when challenged, give unique but reproducible responses. At present, these distinct signatures are commonly generated by physically unclonable functions, or PUFs. These devices provide a straightforward measurement of a physical characteristic of their structure that has inherent randomness, due to imperfections in the manufacturing process[2,3]. These hard-to-predict physical responses can generate a unique identity that can be used for authentication without relying on the secrecy of stored data. However, the classical design of these devices limits both their size and security. Here we show that the extensively studied problematic fluctuations in the current-voltage measurements of resonant tunnelling diodes (RTDs)[4-6] provide an uncomplicated, robust measurement that can function as a PUF without conventional resource limitations. This is possible due to quantum tunnelling within the RTD, and on account of these room temperature quantum effects, we term such devices QUFs – quantum unclonable functions. As a result of the current-voltage spectra being dependent on the atomic structure and composition of the nanostructure within the RTD, each device provides a high degree of uniqueness, whilst being impossible to clone or simulate, even with state-of-the-art technology[7,8]. We have thus created PUF-like devices requiring the fewest resources which make use of quantum phenomena in a highly manufacturable electronic device operating at room temperature. Conventional spectral analysis techniques[9,10], when applied to our QUFs, will enable reliable generation of unpredictable unique identities which can be employed in advanced authentication systems.

Inseparably linking a device to its identity provides a robust building block from which a secure system can be built. Authenticating a device with a protocol, such as certification[11], generally requires the use of a secret key that is typically stored on an integrated circuit (IC). However, it has been shown that invasive and non-invasive attacks have the capability of learning this key, as it must exist in a digital form on the chip, and once compromised an attacker can authenticate themselves as a legitimate device[12]. The IC can be protected by making it tamper-resistant, but this is expensive and difficult. Physically unclonable functions have been proposed to create instance-specific secret keys using physical characteristics of ICs that are never physically stored in the systems memory[13]. The mass-manufacture of components results in random variations during fabrication of the device, which can be exploited for use as PUFs. A number of methods have been proposed to construct a PUF, including; the scattering pattern from an optical medium (illustrated in Fig. 1b)[2], modes in silicon ring oscillators[14], statistical delay variations between nominally identical paths[15], and the power-up state of static random access memories (SRAM) cells[16]. A problem with PUFs based on classical architectures is that they often require significant resources to measure, are not necessarily unclonable, can be emulated, and are susceptible to sophisticated attacks. For instance, an SRAM PUF was successfully cloned within a period of 20 hours by Helfmeier *et al.*[17], an arbiter PUF construction has been shown to be susceptible to modelling[18], whilst implementations of delay based PUF's have demonstrated vulnerabilities to side-channel attacks[19].

The working principle of a PUF is demonstrated in Fig. 1a, a series of unique responses are generated by applying a variety of challenges to the PUF; these challenge-response pairs (CRPs) are used to authenticate the device[13]. A PUF must provide unique, unpredictable and repeatable CRPs and must be practically

[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, M13 9PL, UK.

impossible to clone, even by the manufacturer. Using this approach requires a dedicated online database where the CRPs are recorded and used prior to each communication to authenticate users. Once used, a CRP is erased from the database; each pair in effect forming a one-time-pad[3]. A multiple CRP based authentication system requires a readily available challenge-response database that needs to be large enough to meet security considerations. In an alternative scheme, Koeberl *et al.* proposed a method using a single CRP to authenticate a device[20]. In this system the manufacturer stores a certificate which contains the sole response from the PUF within a signature signed with the manufacturer's private key. When authentication is required, the PUF's response to the challenge is re-measured whilst the signature is verified with the manufacturer's public key to extract the stored response. A check is then performed to determine whether the two values agree.

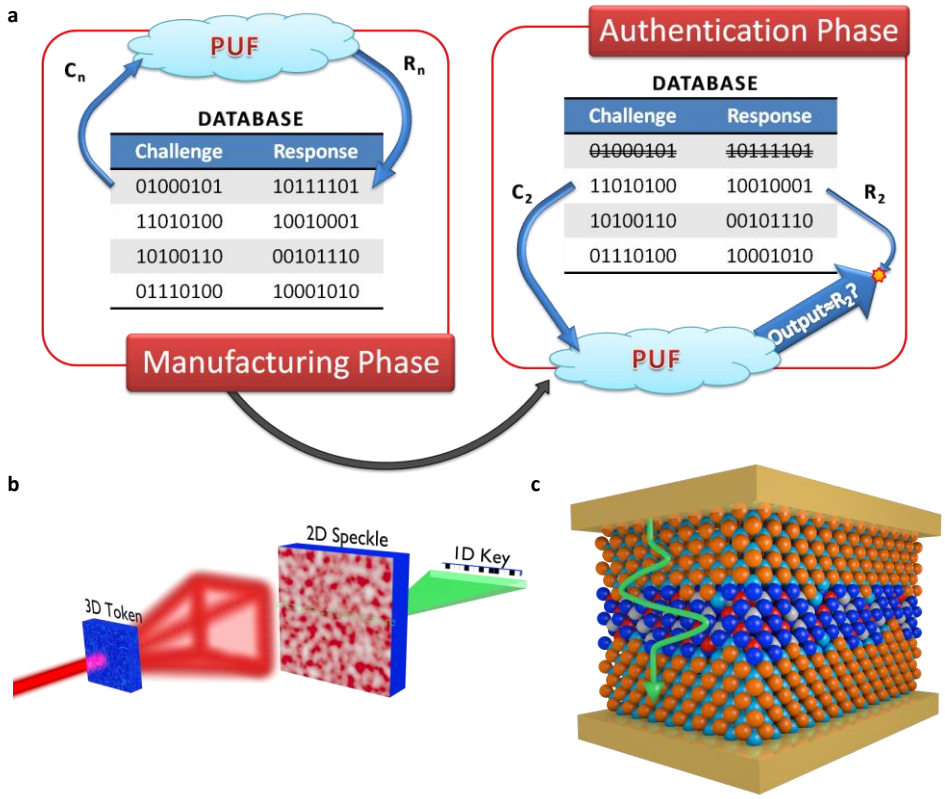

Figure 1| Schematic, working principle and quantum analogue of a physically unclonable function (PUF). a, An example operating protocol for a PUF. A database of challenge (C_n)-response (R_n) pairs is created by the manufacturer and stored online, the user can take a single entry from the database when required to check a device's authenticity. **b,** An optical PUF. The laser is dispersed by a three-dimensional object containing light scattering particles, this causes a two-dimensional speckled image to form, and this pattern can be transformed into a one-dimensional key using hash functions. **c,** Graphic of a conceptual PUF that relies on quantum-mechanical tunnelling through a quantum well containing imperfections (blue region).

As we reduce the size of a system a limit is reached beyond which its behaviour is described by quantum mechanics. Here, the atomic arrangement and composition, of a crystal structure for example, becomes of great importance to the resultant properties[4]. By using a nanostructure containing thousands of atoms, such as the quantum well illustrated in Fig. 1c, a high degree of uniqueness can be achieved due to the inherent random nature of the atomic imperfections at the boundaries of the quantum confining region. Simulating such a structure would require a large amount of computing power and would not be achievable on a reasonable timescale, even with a modest quantum computer[21,22]. At the same time, given the impossibility of copying the device at the atomic level, such technology would be unclonable in the foreseeable future. A quantum well represents the 'least-unique' quantum structure, having only one dimension of confinement, but it enables us to demonstrate the proof-of-principle that we propose. The application of quantum phenomena in a PUF-like architecture provides a means of generating a secret key

[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, M13 9PL, UK.

in an embedded system that can be manufactured with current microelectronic processes. This enables simple system integration with a lower size, weight and power footprint, compared to existing PUF devices. We have coined the term quantum unclonable functions for devices exhibiting these properties. To realise a QUF we use a simple electronic device that can measure phenomenological properties that arise due to quantum confinement. The implementation and measurement of quantum tunnelling can be readily achieved through the use of a resonant tunnelling diode. These are double-barrier structures that allow electrons to pass directly through at voltages corresponding to the energy level within the quantum well lining up with the conduction band minimum. A simple measurement to find the current corresponding to these energies can be achieved by sweeping the voltage through a particular range. As can be seen in Fig. 2c, the Stark shift that results from the application of a voltage (electric field) across the diode causes the position of the energy levels within the quantum well to shift to lower energies, therefore coming into resonance with the conduction band minimum of the system and resulting in a peak in current (transmission probability) which subsequently diminishes as bias is further increased. The resultant room-temperature spectrum from a sample device can be seen in Fig. 2b.

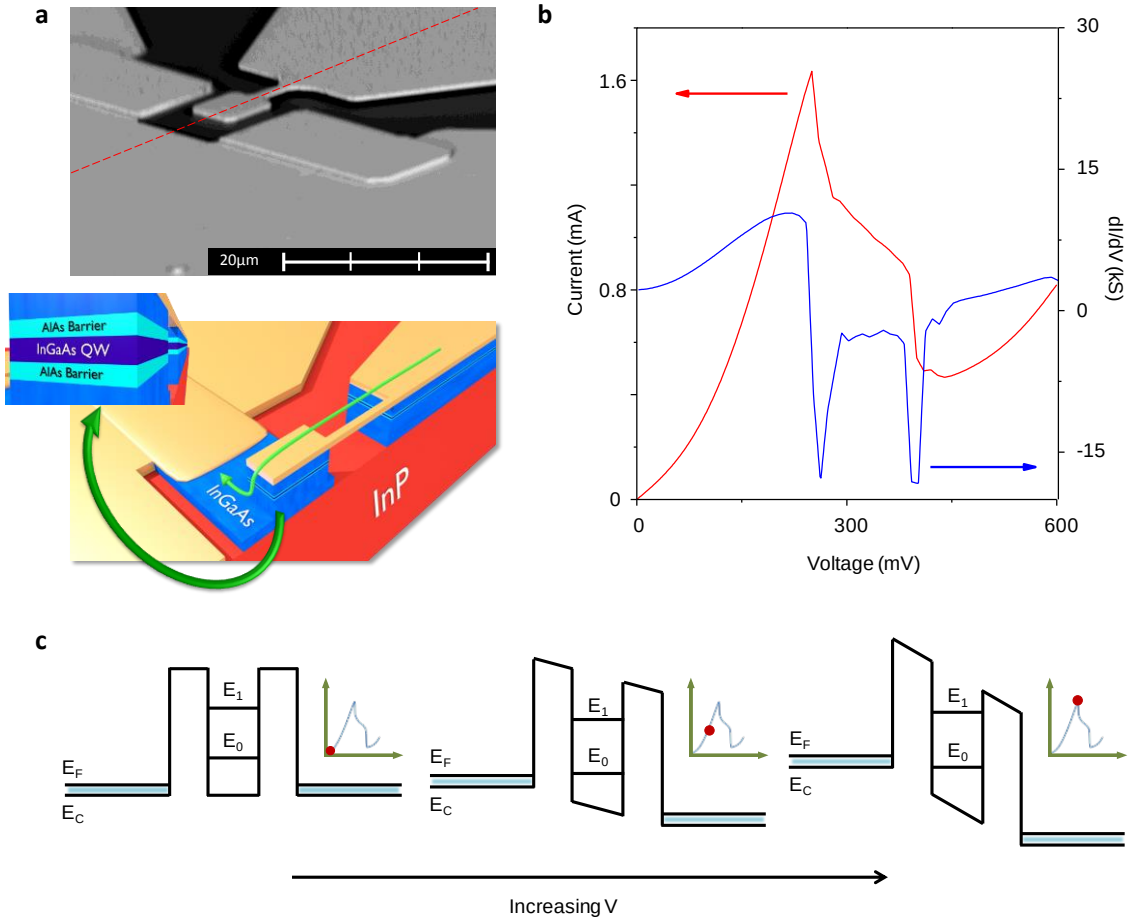

Figure 2| Structure, I-V characteristic and band diagram of a resonant tunnelling diode (RTD). a, Scanning electron microscopy image of a typical device (top) and a rendered counterpart of the cross-section through the red dashed line (bottom) with an inset showing the active region to highlight the important features of the sample; an InGaAs quantum well and barriers made of AlAs **b,** A representative I-V (red) and dI/dV (blue) spectrum from an RTD; the peak in current arises due to the resonance of the confined energy level with the conduction band minimum of the system **c,** Schematic of the E-k structure of the quantum well as the voltage is increased, demonstrating the nature of resonant tunnelling.

For the measurements presented in this letter, RTDs fabricated with mesa sizes of 2x2 µm² were studied; the relatively small area for this geometry of device was found to have greater stability than larger structures (i.e the least drift in repeated I-V measurements). An illustration of the structure used is shown

[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, M13 9PL, UK.

in Fig. 2a, alongside an SEM micrograph; the gold region in the bottom-left represents the back contact whereas the RTD containing mesa is connected via an air bridge to the top contact in the top-right of the images. The important aspects of the structure for this work lie in the region where resonant tunnelling takes place; an InGaAs quantum well sandwiched between two AlAs barriers, shown in the inset to Fig. 2a.

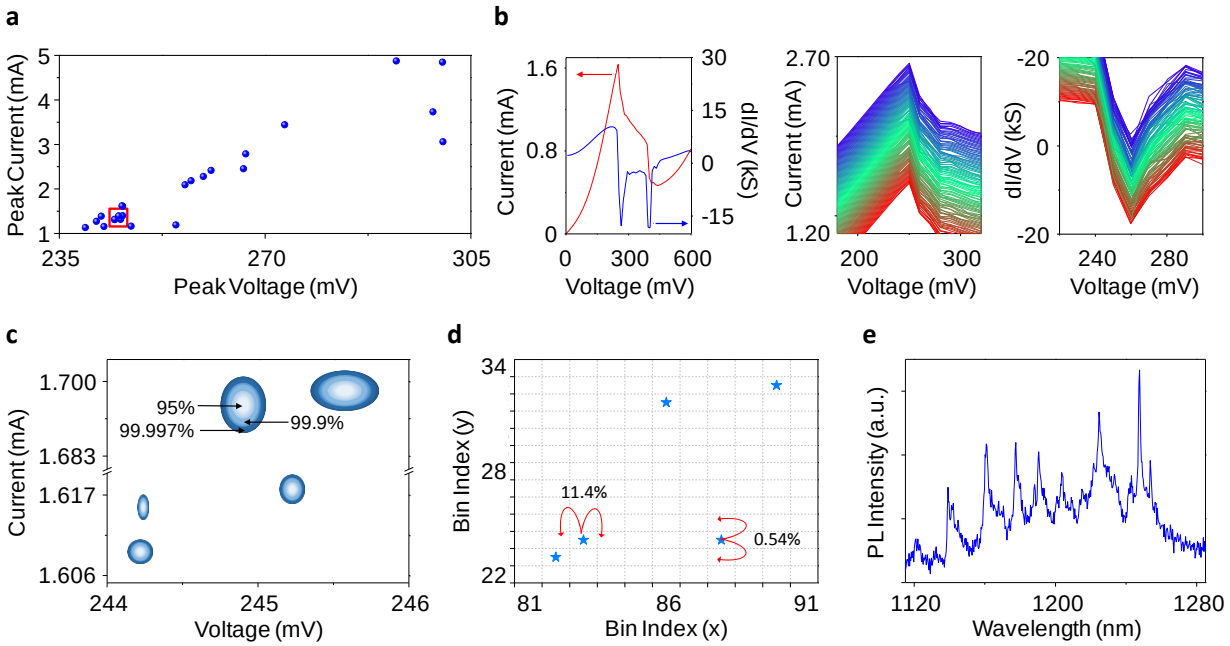

Figure 3| Uniqueness and reproducibility performance of a quantum unclonable function (QUF). a, Positions of associated peak voltages and currents for 26 devices manufactured to have identical characteristics. **b,** I-V and dI/dV curve of a single device (left); 100 measurements of I-V (centre) and dI/dV (right) from the same device (offset for clarity). **c,** Zoomed-in view of the highlighted section in **a** showing 95, 99.9 and 99.997% confidence ellipses of the 5 devices tested that lie the closest together. **d,** Probability of a device falling into another bin on x/y axis for the same area as in **c**. **e,** Photoluminescence spectrum from a sample containing quantum dots.

To justify the use of quantum tunnelling as a measure of uniqueness, we inspected 26 devices manufactured with identical features, namely a rounded mesa connected to a 3µm air bridge. Each device's average current-voltage characteristic was measured and a subsequent Gaussian fit was applied to find the position of the peak current and voltage, plotted in Fig. 3a. From this figure it can be noted that there is a large scope of available peak positions, ranging by approximately 70 mV in voltage and 4 mA in current, thus providing a low collision probability. It can also be recognised that the position of each device within this region is unique, although the highlighted area at the lower end of the spectrum seems to have overlapping devices, this is an artefact of the symbol size. Fig.'s 3c and 3d investigate this aforementioned area; the former shows a plot of the true precision of the calculated average using ellipses to represent different confidence bounds. These were extracted from the spread of measurements. Upon examination of Fig. 3c, it can be seen that there is no overlap between devices with a 99.997% certainty; this reiterates the fact that all 26 of the measured devices are distinctive and so could be used to extract a unique identity. The precision of the average to these confidence ellipses was found by using the standard errors in voltage as the semi-major axis and standard errors in current as semi-minor axis. The ellipses confidence limits of 95%, 99.9% and 99.997% correspond to using 1.96, 3.09 and 3.99 standard errors respectively.

The motivation behind re-plotting the data from Fig. 3c on axes represented by bin indices in Fig. 3d becomes apparent when considering a realistic implementation of a device. In a practical execution, a unique number would be extracted depending on bin position. We have split both axes into 256 bins and considered the probability of a device changing its bin index when re-measured; this has been found to be

[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, M13 9PL, UK.

11.4% on the x-axis and 0.54% on the y-axis. These probabilities are largely dependent on the number of bins on a particular axis, if it is split into more bins then the probability of shifting bins would be greater, but the number of different devices that could be extracted would be improved, whereas using fewer bins decreases this probability but allows the extraction of fewer devices.

Measurements need to be reproducible when considering real world implementation; the results shown in Fig. 3b were taken to test the stability of these devices. The left figure is the average I-V characteristic for one of the RTDs as we saw previously in Fig. 2, from this the associated peak in both the current (centre) and differential current, or gradient of the negative differential resistance region (right) vs. voltage has been displayed in more detail. The two graphs show data from 100 repeated I-V measurements taken from the device; each graph represents a unique number that can be extracted. The peak position of each measurement has been found to lie within at least two standard errors of the calculated average in both measurement axes, a good indication to the high calibre of robustness we expect from such devices.

Taking the current range spanned by the devices measured here, and the average uncertainty in the peak position, measured with high confidence, we can extrapolate that the QUF structure introduced here could provide of the order of 10^3 unique identities. For practical applications, such a number would be easily increased by combining multiple devices in an array. As the array size increases the number of unique identities available scales exponentially.

Alongside this, the use of more complex three-dimensional nanostructures should also significantly increase the device uniqueness. As an example of such nanostructures, quantum dots typically have many electron and hole confinement levels, as illustrated by the rich photoluminescence spectrum emitted from a few GaSb quantum dots shown in Fig. 3e. RTD's containing single, or a few, quantum dots reflect this increase in the number of confined states with an increased number of peaks in their dI/dV curves[23-25]. Each of these peaks, fitted individually and combined, forms a unique key for the device. The benefit of applying quantum dots within a resonant tunnelling structure is the practicality of such an electronic room-temperature measurement (a necessity for PUFs), unlike micro-PL measurements which require sub-20K temperatures and a complicated optical system. Moreover, as the number of dots in a device does not need to be reproducible, fabrication using self-assembly techniques are well suited to these devices.

To conclude, while inhomogeneity in the fabrication of nanostructures often leads to unpredictable behaviour of the final device, which is undesirable in most applications, we have proposed and demonstrated a potential use for the quantum behaviour of atomically irreproducible systems. The devices we have presented, based around 1D quantum structures, afford a secure bit density of 2.5 bits/μm^2. This is twice the value of state of the art classical PUF's[26], and we expect it to increase significantly for devices containing structures that provide three-dimensional quantum confinement. There is strong indication that these devices can be seamlessly integrated into embedded electronic systems to provide robust unique identities that would require atomic level engineering to clone.

Methods

The RTD devices were fabricated from an InGaAs/AlAs double-barrier structure grown by molecular beam expitaxy on an InP substrate. The details of this are given in reference [27]. To fabricate the RTDs, a top contact was first defined using conventional i-line optical lithography. A non-alloyed ohmic contact method was employed, where titanium (50 nm) and gold (250 nm) were deposited onto the surface of the highly doped cap layer by thermal evaporation. The top metal itself acted as a hard mask for a subsequent mesa etch. A reactive-ion etching (RIE) process using a mixture of methane (CH_4) and hydrogen (H_2), with an etch rate of 21 nm/minute, was implemented in order to produce anisotropic side-walls to the bottom contact

[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, M13 9PL, UK.

layer, in preparation for the bottom metal contact deposition. Just before the bottom metal contact process took place, a non-selective orthophosphoric-based (H_2O:H_3PO_4:H_2O_2 = 50:3:1) wet-etch with a etch rate of 90 nm/minute was used to etch away 200 nm of epilayers down to the surface of the InP to completely isolate neighbouring devices. The 5 minutes wet-etch also simultaneously provided the necessary undercut for the air-bridge formation. Finally, the bottom ohmic contact was formed by thermal evaporation of Ti/Au (50 nm/500 nm).

The devices measured were not precisely 2x2µm², as the fabrication process tends to resulted in round-shaped mesas, however this is a minor detail as the measurements made are much more sensitive to the variations in the 1D confinement potential of the well than its profile. All measurements were taken at 300K using a Keithley 2400 source measure unit connected to a Wentworth Laboratories Ltd. SPM197 probe station using two 1.25" tungsten probes with 1µm tip radii. For each RTD, a voltage sweep between 0 and 1V was performed with the current being measured in voltage steps of 10mV; this measurement was repeated 100 times per device. The voltage sweep was performed as follows: the voltage source is initially set to a value of 0V, a measurement delay of 80ms is used to allow the source to settle to the given source value and subsequently the average current measurement corresponding to this voltage was taken over 60ms, finally the source voltage is stepped up by 10mV and this whole process is repeated for the next value. Because of the nature of two probe measurements, the evaluated current-voltage characteristics showed oscillations in the peak values due to the probes making intermittent contact with the surface (causing changes in resistance), therefore the I-V curves were re-taken until a good contact was achieved. The voltage and current ranges were also key considerations; if probed above 1V or allowed to rise above 10mA the RTDs broke down and then showed uncharacteristic ohmic-like behaviour. Finally, it is important to note that during 100 measurements, it was clear that some devices were reaching a critical temperature, which resulted in small chemical changes that seemed to cause a slight shift in the peak I-V. This particular aspect could be useful when considering a realistic implementation, as it would enable the device to be effectively 'reset' so that it exhibited a distinct new signal.

[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, M13 9PL, UK.

Acknowledgements This work is supported by the Royal Society through a University Research Fellowship held by R.J.Y. J.R. is supported by the EPSRC 'NOWNANO' DTC. M.M. also acknowledges the support of the Science and Technologies Facilities Council (STFC).

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

Author Information Correspondence and requests for materials should be addressed to R.J.Y. (r.j.young@lancaster.ac.uk).

References

1. Guin, G. *et al*. Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. *in Proc. IEEE* **102**, 1207-1228 (2014).
2. Pappu, R., Recht, B., Taylor, J. & Gershenfeld, N. Physical one-way functions. *Science* **297**, 2026-2030 (2002).
3. Horstmeyer, R., Judkewitz, B., Vellekoop, I. M., Assawaworrarit, S. & Yang, C. Physical key-protected one-time pad. *Scientific Reports **3**,* 3543 (2013).
4. Tsuchiya, M. & Sakaki, H. Dependence of resonant tunneling current on well widths in AlAs/GaAs/AlAs double barrier diode structures. *Appl. Phys. Lett.* **49**, 88 (1986).
5. Lin, Y., van Rheenen, A. D. & Chou, S. Y. Current fluctuations in double-barrier quantum well resonant tunneling diodes. *Appl. Phys. Lett.* **59**, 1105 (1991).
6. Ng, S., Surya, C., Brown, E. R. & Maki, P. A. Observation of random-telegraph noise in resonant-tunneling diodes. *Appl. Phys. Lett.* **62**, 2262 (1993).
7. Wegscheider, W., Schedelbeck, G., Abstreiter, G., Rother, M. & Bichler, M. Atomically precise GaAs/AlGaAs quantum dots fabricated by twofold cleaved edge overgrowth. *Phys. Rev. Lett.* **79**, 1917-1920 (1997).
8. Fölsch, S., Martinez-Blanco, J., Yang, J., Kanisawa, K. & Erwin, S. C. Quantum dots with single-atom precision. *Nature Nanotechnol.* **9**, 505-508 (2014).
9. Schwartz, L. M. Digital method of spectral peak analysis. *Anal. Chem.* **43**, 1336-1338 (1971).
10. Von Meerwall, E. Automatic peak analysis on minicomputers. *Comput. Phys. Commun.* **5**, 309-313 (1973).
11. Simmons, G. J. *Contemporary Cryptology: The Science of Information Integrity* (IEEE Press, New Jersey, 1994).
12. Barenghi, A., Breveglieri, L., Koren, I. & Naccache, D. Fault injection attacks on cryptographic devices: theory, practise and countermeasures. in *Proc. IEEE* **100**, 3056-3076 (2012).
13. Suh, G. E. & Devadas, S. Physical unclonable functions for device authentication and secret key generation. in *Proc. of the 44th Annual Design Automation Conference, 9-14 (IEEE 2007).*
14. Gassend, B., Clarke, D., van Dijk, M. & Devadas, S. Silicon physical random functions. in *Proc. of the 9th ACM Conference on Comput. and Commun. Security*,148-160 (CCS 2002).
15. Lim, D. *et al.* Extracting secret keys from integrated circuits. *IEEE Transactions on VLSI Systems* **13**, 1200-1205 (2005).
16. Holcomb, D. E., Burleson, W. P. & Fu, K. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Transactions on Computers* **58**, 1198-1210 (2009).
17. Helfmeier, C., Nedospasov, D., Boit, C. & Seifert, J. Cloning physically unclonable functions. *IEEE International Symposium on Hardware-Oriented Security and Trust,* 1-6 (IEEE 2013).

[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, M13 9PL, UK.

18. Lee, J. W. *et al.* A technique to build a secret key in integrated circuits for identification and authentication application. *IEEE Symposium on VLSI Circuits,* 176-179(IEEE 2004).
19. Ruhrmair, U. & van Dijk, M. PUFs in security protocols: attack models and security evaluations. *IEEE Symposium on Security and Privacy*, 286-300(IEEE 2013).
20. Koeberl, P., Li, J., Rajan, A. Vishik, C. & Wu, W. A practical device authentication scheme using SRAM PUFs. *Proc. of the 4th International Conference on Trust and Trustworthy Computing,* 63-77 (Springer 2007).
21. Cirac, J. I. & Zoller, P. Goals and opportunities in quantum simulation. *Nature Phys.* **8**, 264-266 (2012).
22. Buluta, I. & Nori, F. Quantum Simulators. *Science* **236**, 108-111 (2009).
23. Li, P. W., Kuo, D. M. T. & Hsu, Y. C. Photoexcitation effects on charge transport of Ge quantum-dot resonant tunneling diodes. *Appl. Phys. Lett.* **89**, 133105 (2006).
24. Lai, W., Kuo, D. M. T. & Li, P. Transient current through a single germanium quantum dot. *Physica E* **41**, 886-889 (2009).
25. Chen, K., Chien, C. & Li, P. Precise Ge quantum dot placement for quantum tunneling devices. *Nanotechnol.* **21**, 055302 (2010).
26. Maes, R. *Physically Unclonable Functions* (Springer, Berlin, 2013).
27. Zawawi, M. A. M., KaWa, I., Sexton, J. & Missous, M. Fabrication of sub-micrometer InGaAs/AlAs resonant tunneling diode using a tri-layer soft reflow technique with excellent scalability. *IEEE Transactions on Electron Devices*. **61**, 2338-2342 (2014).

[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, M13 9PL, UK.