Atomic-scale Authentication with Resonant Tunneling Diodes

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

ABSTRACT

The room temperature electronic characteristics of resonant tunneling diodes (RTDs) containing AlAs/InGaAs quantum wells are studied. Differences in the peak current and voltages, associated with device-to-device variations in the structure and width of the quantum well are analyzed. A method to use these differences between devices is introduced and shown to uniquely identify each of the individual devices under test. This investigation shows that quantum confinement in RTDs allows them to operate as physical unclonable functions.

INTRODUCTION

Inseparably linking a device to its identity provides a robust building block from which a secure system can be built. Authenticating such a device with a protocol, for example certification [1], generally requires the use of secret keys stored in integrated circuits. It has been shown that invasive and non-invasive attacks have the capability of learning these keys however, as they exist in a digital form on the chip. After being compromised, an attacker can pose as a trustworthy party and successfully authenticate themselves. The devices can be protected by making them tamper-resistant, but this requires significant resources. Physical unclonable functions (PUFs) [2] have been proposed to create instance-specific secret keys using the random physical characteristics of ICs that are never stored in the system's memory. 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 different categories of PUFs have emerged including; delay PUFs [3], SRAM PUFs [4], butterfly PUFs [5], and bistable ring PUFs [6]. Existing PUFs suffer from a number of limitations, they often require significant resources to measure, are clonable with advanced manufacturing techniques, can be emulated, and are susceptible to sophisticated attacks. For instance, an SRAM PUF was successfully cloned within a period of 20 hours [7]. In this paper resonant tunneling diodes (RTDs) are studied, with the variations in the quantum confinement they provide used to realize a PUF. The relative merits of this class of quantum confinement PUF (QC-PUF) are discussed.

As the size of an electronic system decreases there is a limit beyond which quantum mechanics describes its behavior. In this regime, the atomic arrangement of a crystal structure becomes important to the properties of the system, such as quantum confinement [8]. Nanostructures containing thousands of atoms, such as quantum dots and wells, are highly unique, due to the inherent random nature of the atomic imperfections. Simulating these structures from first principles requires a large amount of computation power and is not achievable on a reasonable timescale [9]. Additionally, as it is not possible to copy the device at the atomic level [10,11], this technology will be unclonable for the foreseeable future. In this

work the application of quantum confinement in a PUF-like architecture is studied, as a means to generate a secret key in an embedded system.

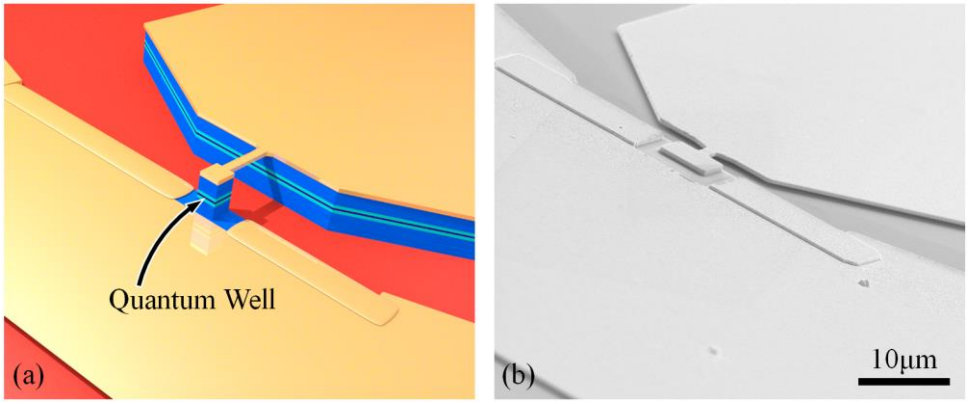

Figure 1. (a) An illustration of the resonant tunneling diode structure with a false z-scale to highlight the InGaAs/AlAs quantum well. (b) A scanning electron microscope image of a typical device.

EXPERIMENT

The structure of the RTD devices used in this work is illustrated in figure 1(a). They were fabricated from an InGaAs/AlAs double-barrier structure grown by molecular beam epitaxy on an InP substrate. Further details of the structure can be found in [12]. They were processed by first defining a top contact 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) was implemented in order to produce anisotropic side-walls to the bottom contact layer, in preparation for the bottom metal contact deposition. Before the bottom metal contact was formed, a non-selective wet-etch was used to remove the epilayers to reveal the underlying InP to isolate neighboring devices. This wet-etch also undercut the air-bridge, as shown in the figure. Lastly, the bottom ohmic contact was formed by thermal evaporation of Ti/Au (50 nm/500 nm). Figure 1(b) shows a scanning electron microscope image of a typical device after fabrication and processing.

For electronic measurements, nominally identical RTDs fabricated with mesa areas of ~4 μm², were selected. To characterize variations in the quantum confined energy levels induced by imperfections in the well [13-16] a source measure unit connected to a probe station was used to obtain current-voltage curves at room temperature. A voltage sweep from 0 V to 1 V was taken in steps of 10 mV for each diode at room temperature to record a current spectrum. A spectrum from a sample device is shown in the inset to figure 2. This measurement was repeated 100 times per device to assess the reproducibility of the measurements. The average current-voltage characteristic for 26 devices were measured, and then a Gaussian fit was used to extract the peak current and voltage [17]. The results from this are shown in figure 2. The errors in the measurement are extremely small and most are obscured by the symbol size, thus the bottom-right inset shows a zoomed-in view of the red boxed area with errors displayed. Each point has been shown with two standard error bars in both the voltage and current axis.

For implementation in a digital security system the output from the peak fitting procedure should be converted into a key. To achieve this, the results from the highlighted box in figure 2 have been replotted in figure 3 with the axes representing bin indices. The rationale for this comes from the necessity of extracting a unique number in practical implementation, where this unique number is extracted from the bin indices and not the straightforward voltage and current values. The distribution of all results has been split into 256 bins, with the highlighted region falling between bins 80 and 90 (voltage axis) and 20 and 35 (current axis). The probability of a device changing its bin index when re-measured can be calculated using the errors in the measurement. These probabilities are dependent on the number of bins chosen for each axis.

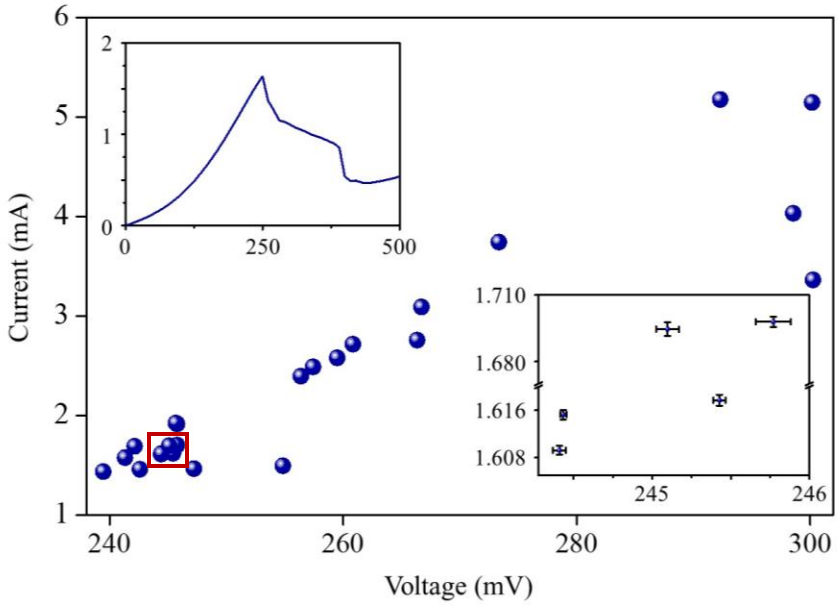

Figure 2. Peak voltage vs. current for 26 individual devices indicating the spread in results. The top-left inset shows typical measurement for a single device whilst the bottom-right inset displays the boxed region in finer detail.

DISCUSSION

The origin of the unique I-V measurements within an RTD comes from the differences in the average layer thickness of the barriers and quantum well resulting from imperfect MBE growth at these important interfaces. This is exaggerated in our case as binary and ternary layers are adjacent in the active region, resulting in a larger interfacial roughness. Reference [18] quantifies how an imperfect interface can change the resulting I-V, stating that interfacial variations of the order of 1 monolayer can change the I-V characteristics by 270%. This can easily be achieved by manipulating the MBE growth for added uniqueness.

To utilize quantum confinement in an RTD as a PUF, the measurement needs to be robust and repeatable. The results shown in figure 2 show the average result from fitting 100 repeated I-V measurements taken from each device. 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 caliber of robustness expected of test devices.

From figure 2 there is a broad range of peak positions available, spanning roughly 70 mV in voltage and 4 mA in current. This gives a low probability of collision. It can also be recognized that the position of each device within this region is unique, although the area at the lower end of the spectrum seems to have overlapping devices, this is an artifact of the symbol size. Upon magnification, there is no overlap between devices with a 99.997% certainty. All 26 of the measured devices are distinct and the measurements made from them could be used to extract unique identities. Using the current range of the devices and the uncertainty in the measurements, the maximum number of QC-PUF devices providing unique identities is estimated to be of the order of 10^3. For practical applications, such a number would be easily increased by combining multiple devices in an array [19], by connecting them programmatically to form a strong PUF. As the array size increases the number of unique identities available scales exponentially. It is also possible to use three-dimensional nanostructures, rather than quantum wells, which would significantly increase the device uniqueness [20-22]. Each of these peaks, fitted individually and combined, could form a component of the unique key for the device.

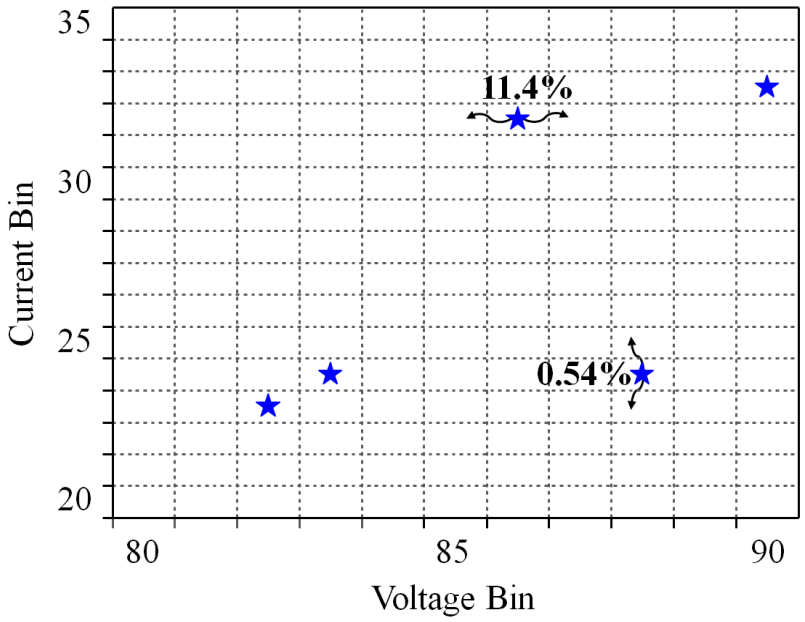

Figure 3. A subsection of the data from figure 2 replotted on scales with bins, to indicate how the quantum confinement physical unclonable function's output could be digitized. The percentages indicate the probability of a measurement 'hopping' one bin along the two axes.

CONCLUSIONS

In conclusion, the use of quantum behavior to uniquely identify devices, through inherent atomic imperfections, has been proposed and demonstrated. The devices presented contained a one dimensional quantum structure and gave a secure bit density of 2.5 bits/μm^2. This is roughly twice the value of state-of-the-art classical PUFs. This is expected to increase significantly for devices containing structures providing three-dimensional quantum confinement. These devices can be seamlessly integrated into embedded electronic systems to provide robust unique identities, and they would require atomic level engineering to clone.

ACKNOWLEDGMENTS

This work is supported by the Royal Society through a University Research Fellowship (grant UF110555) held by R. J. Young. J. Roberts is supported by the EPSRC 'NOWNANO' DTC (grant EP/L01548X/1). M.M. is supported by the Science and Technologies Facilities Council (STFC)

REFERENCES

1. *Contemporary Cryptology: The Science of Information Integrity*, ed. G. J. Simmons (IEEE Press, 1994).
2. R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, *Science* **297**, 2026 (2002).
3. B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, *Proceedings of the Computer and Communications Security Conference*, 148 (2002)
4. D. E. Holcomb, W. P. Burleson, and K. Fu, *Proceedings of the Conference on RFID Security*, **7** (2007).
5. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, and P. Tuyls, *IEEE International Workshop on Hardware Oriented Security and Trust*, 67 (2008).
6. Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and Ulrich Ruhrmair, *IEEE International Symposium on Hardware-Oriented Security and Trust*, 134 (2011).
7. C. Helfmeier, D. Nedospasov, C. Boit, and J. Seifert, *IEEE International Symposium on Hardware-Oriented Security and Trust*, 1 (2013).
8. M. Tsuchiya, and H. Sakaki, *Appl. Phys. Lett.* **49**, 88 (1986).
9. J. I. Cirac, and P. Zoller, *Nature Phys.* **8**, 264 (2012).
10. W. Wegscheider, G. Schedelbeck, G. Abstreiter, M. Rother, and M. Bichler, *Phys. Rev. Lett.* **79**, 1917 (1997).
11. S. Fölsch, J, Martinez-Blanco, J. Yang, K. Kanisawa, and S. C. Erwin, *Nature Nanotech.* **9**, 505 (2014).
12. M. A. M. Zawawi, I. KaWa, J. Sexton and M. Missous, *IEEE Transactions on Electron Devices*. **61**, 2338-2342 (2014).
13. V. A. Wilkinson, M. J. Kelly, and M. Carr, *Semicond. Sci. Technol.* **12**, 91 (1997).
14. M. J. Kelly, *Semicond. Sci. Technol.* **15**, 79 (2000).
15. P. Dasmahapatra, J. Sexton, M. Missous, C. Shao, and M. J. Kelly, *Semicond. Sci. Technol.* **27**, 085007 (2012).
16. C. Shao, J. Sexton, M. Missous, and M. J. Kelly, *Electronics Letters* **49**, 10 (2013).
17. J. Roberts et al., *Sci. Rep.* **5**, 16456 (2015).
18. M. Missous, M. J. Kelly and J. Sexton. *IEEE Electron Device Letters* **36**, 6 (2015).
19. U. Rürrmair, *Lecture Notes in Computer Science* **6052**, 328 (2010).
20. P. W. Li, D. M. T. Kuo, and Y. C. Hsu, *Appl. Phys. Lett.* **89**, 133105 (2006).
21. W. Lai, D. M. T. Kuo, and P. Li, *Physica E* **41**, 886 (2009).
22. K. Chen, C. Chien, and P. Li, *Nanotechnol.* **21**, 055302 (2010).