Molecular-scale hardware encryption using tunable self-assembled nanoelectronic networks

Venkataraman, A., Amadi, E., & Papadopoulos, C.

2022

micro

MDPI

Article

Molecular-Scale Hardware Encryption Using Tunable Self-Assembled Nanoelectronic Networks

Anusha Venkataraman, Eberechukwu Amadi and Chris Papadopoulos *

Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 1700 STN CSC, Victoria, BC V8W 2Y2, Canada; anushav@uvic.ca (A.V.); eamadi@uvic.ca (E.A.)
* Correspondence: papadop@uvic.ca

Abstract: Nanomaterials are promising alternatives for creating hardware security primitives that are considered more robust and less susceptible to physical attacks compared to standard CMOS-based approaches. Here, nanoscale electronic circuits composed of tunable ratios of molecules and colloidal nanoparticles formed via self-assembly on silicon wafers are investigated for information and hardware security by utilizing device-level physical variations induced during fabrication. Two-terminal electronic transport measurements show variations in current through different parts of the nanoscale network, which are used to define electronic physically unclonable functions. By comparing different current paths, arrays of binary bits are generated that can be used as encryption keys. Evaluation of the keys using Hamming inter-distance values indicates that performance is improved by varying the ratio of molecules to nanoparticles in the network, which demonstrates self-assembly as a potential path toward implementing molecular-scale hardware security primitives. These nanoelectronic networks thus combine facile fabrication with a large variety of possible network building blocks, enabling their utilization for hardware security with additional degrees of freedom that is difficult to achieve using conventional systems.

Keywords: nanomaterials; self-assembly; hardware security; physically unclonable functions

Citation: Venkataraman, A.; Amadi, E.; Papadopoulos, C. Molecular-Scale Hardware Encryption Using Tunable Self-Assembled Nanoelectronic Networks. *Micro* **2022**, *2*, 361–368. https://doi.org/10.3390/micro2030024

Academic Editor: Laura Chronopoulou

Received: 16 May 2022
Accepted: 17 June 2022
Published: 21 June 2022

1. Introduction

Nanoscale electronic devices based on molecules are being developed in order to potentially overcome limitations in conventional electronics scaling and provide functions "beyond CMOS" [1–3]. These molecular electronic circuits exhibit ease of fabrication, low cost, and a high degree of tunability [4–6]. Hardware security is an emerging important area of application for nanomaterials, wherein their unique properties and functionality may enable utilization for future advanced security primitives and applications in ubiquitous computing and information technologies [7]. Carbon nanostructures, quantum dots, and colloidal nanoparticles are all being investigated for use in information and hardware security solutions [8–10].

Conventional security primitives typically rely on different mathematical or algorithmic protocols. For example, pseudorandom number generators are often used for generating encryption keys to protect confidential information. However, such solutions are typically slow, energy intensive, and often vulnerable to side-channel and physical attacks (e.g., radiation, high temperatures) [7,11]. To address these challenges, device-level hardware security approaches that consume less energy with smaller performance overhead are being investigated for general and emerging security requirements that utilize inherent physical randomness and device imperfections introduced during fabrication or operation. Examples include hardware-based true random number generators (TRNGs) that use thermal noise to generate random outputs, and cryptographic key generation using physically unclonable functions (PUFs) from intrinsic physical imperfections [12,13]. Most cryptographic primitives try to generate unique keys that can authenticate the required

information, thus preventing security threats [14]. One example is silicon-based PUFs based on local device mismatches such as random dopant fluctuation arising from stochastic variations during processing. While promising, such CMOS-based PUFs can also often be susceptible to supply voltage noise and temperature fluctuations that could allow for data tampering, counterfeiting, and information leakage [15]. In addition, the relative ease with which CMOS devices can be modeled and simulated allows exploitation of conventional semiconductor process variations and potential exposure to so-called modeling attacks [16].

An alternative path to hardware security primitives is based on functional nanomaterials, which can enhance performance and is considered more robust and less susceptible to attacks compared to standard CMOS-based security primitives [17]. Functional nanomaterials show unique capabilities and new degrees of freedom relevant to security such as nonlinear input–output response characteristics, inherent tunability, and non-volatility [16]. The resulting nanostructured devices can be tailored for variability, reconfigurability, randomness, and resilience against reverse engineering [11], which enables applications requiring PUFs, TRNGs, anti-counterfeit measures, side-channel leakage masking, and resistance to tampering: Metallic nanoparticles with unique optical properties for generating PUFs can serve as tamper-evident sensors and "nanofingerprints" for anti-counterfeit applications [8,10,18,19]; PUFs and TRNGs using carbon nanotube structures and electronic devices are promising for future security applications due to good chemical stability, excellent electronic properties, and low-cost solution-based processing [9,20–22]; lastly, nanomechanical structures [23] and nanostructured memristors [24] have also shown promise for hardware security applications.

Self-assembled gold nanoparticle-molecular networks are another class of structures with potential for hardware security primitives, including the generation of random encryption keys based on PUFs. Previous work has shown interesting behavior in self-assembled networks such as negative differential resistance (NDR) [6,25], hysteresis [6], rectification [26], and switching phenomenon [27]. Network mismatches and disorder during self-assembly could also lead to randomized metal–molecular connections that are advantageous for generating encryption keys [21,22]. In this work, we present results using self-assembled metal–molecular networks formed between multiple electrodes on silicon substrates that are utilized as electronic PUFs to generate sequences of random bits for encryption keys. Instead of relying solely on stochastic processes, we employ a tunable self-assembly process to vary the network configuration and thus introduce an additional degree of freedom for hardware security and encryption at the molecular level: Modifications to the networks based on tunable molecule-to-nanoparticle ratios lead to unique current–voltage (*I*–*V*) profiles that demonstrate their use for information security applications.

2. Materials and Methods

Thirty nm diameter citrate-stabilized colloidal gold nanoparticles; 1,4-benzenedithiol (BDT) and 1,9-nonanedithiol (NDT) molecules were purchased from Sigma-Aldrich. NaOH pellets were purchased from EMD. All chemicals were used as received. Pure ethanol from Greenfield Global and deionized water were used as solvents. Photo-lithographically patterned gold electrodes (40 nm gold, with a thin adhesion layer) on oxidized silicon wafers (100 nm SiO_2), were used as substrates for *I*–*V* measurements. The electrode spacing varied between 1 and 2.5 μm.

Self-assembled gold nanoparticle-molecular network films were made according to [28,29], with certain modifications [6,30]. In brief, the ratio N_{molecule}:N_{particle} (where N_{molecule} is the number of dithiol molecules and N_{particle} is the number of colloidal gold particles) was varied to control the concentration and arrangement of molecule-to-gold interconnections in the resulting networks. In order to achieve the desired N_{molecule}:N_{particle} ratio, an ethanolic solution of molecules of the appropriate molarity was first prepared. Similarly, a colloidal gold suspension of a given concentration was prepared using dilute NaOH and then mixed with an equal volume of molecule solution and incubated at 4 °C for 24 h. To obtain different N_{molecule}:N_{particle} ratios, this synthesis procedure was repeated

using modified concentrations of molecular solution. Following incubation, μL drops of the resulting gold nanoparticle–molecular suspension were deposited on the patterned electrodes and allowed to dry in ambient conditions to form self-assembled films before electrical characterization.

I–V data were obtained using a Janis probe station and tungsten tips connected to a precision characterization system (Keithley 4200-SCS). The networked films were imaged with an Olympus BXFM optical microscope and Nanonics Multi-View 1000 AFM with pulled glass fiber tips (10 nm nominal diameter) in intermittent contact mode.

The low-bias electrical response of the networks was modeled with the LTspice circuit simulation software following earlier work [30]: The networks were first abstracted into a network of interconnected resistors corresponding to the dimensions of the nanoparticle–molecular networks obtained from microscope images. The gold–gold nanoparticle connections were assumed to have the quantized value of resistance, 12,907 Ω. The number and location of gold–molecule connections in the network were varied using a pseudorandom number generator that assigned either the quantized inter-particle contact resistance or the appropriate molecule resistance (based on previous work) [31–34]. The network was built with 8 electrodes to contact and probe the molecular network at various points, analogous to the experimental setup.

3. Results and Discussion

Figure 1 shows a schematic of the overall process flow used to generate binary keys using the self-assembled metal–molecular networks: A unique current profile (Figure 1a) is generated based on the different transport paths through the thin film networks consisting of interconnected colloidal gold nanoparticles and thiolated molecules, determined by the electrode pairs shown in Figure 1b. The current vs. electrode pair data is then used to define a PUF for the creation of a sequence of bits that generate binary keys (Figure 1c). The molecule type and ratio of molecules to nanoparticles can be used to vary network morphology by directing the self-assembly process, and thus the number of gold–molecular vs. gold–gold connections and their distribution can be modified in the resulting nanoelectronic circuit [6,30] (schematic, Figure 1c).

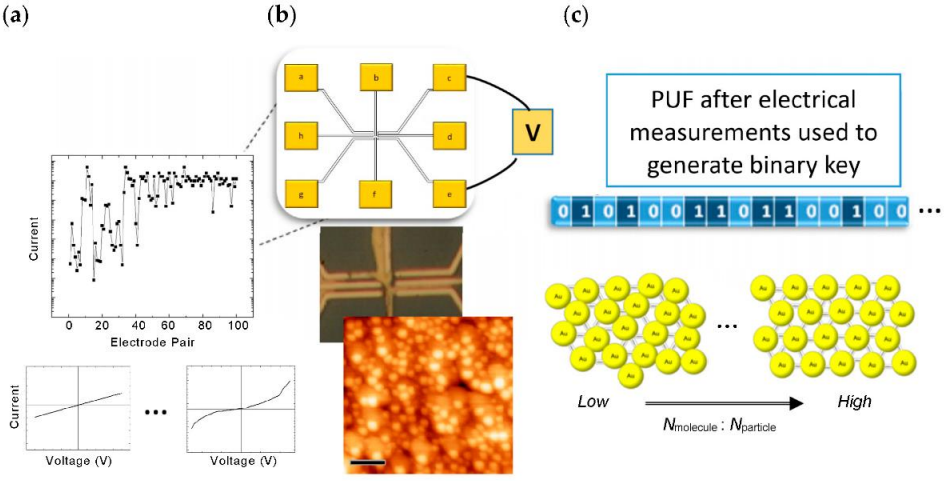
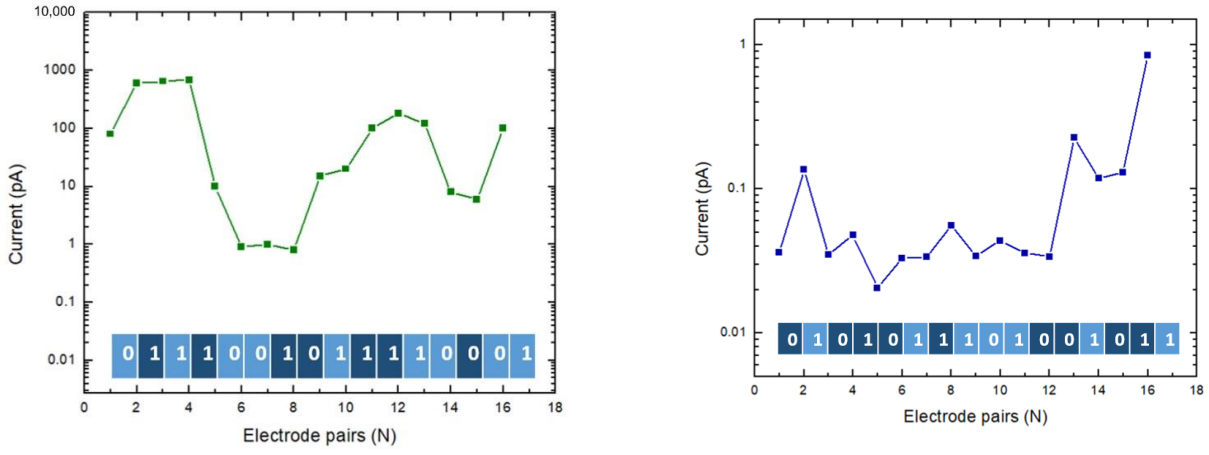


Figure 1. (**a**) Illustration of network film current profile (0.5 V) obtained using *I–V* curves for different electrode pair combinations probed via two-terminal electrical measurements (typical *I–V* data plots shown). (**b**) Schematic of patterned electrode configuration used to probe networks and optical microscope image of patterned gold electrodes after depositing gold nanoparticle–molecular network. AFM image shows typical self-assembled network film formed between contacts on SiO_2/Si substrate (scale bar equals 100 nm). (**c**) Illustration of binary key generation based on unique current profiles determined by ratio of molecules to colloidal gold particles in the network during the self-assembly process. Schematic shows idealized molecular interconnections between particles in the network for different ratios (not to scale).

Several nanoscale network samples with different dithiol molecules (BDT and NDT), acting as linkers between gold nanoparticles, and $N_{molecule}$:$N_{particle}$ ratios were fabricated for electrical characterization. Typical low-bias two-terminal *I*–*V* characteristics (up to ~0.5 V) were consistent with prior work [30,35–37], while nonlinearities such as NDR and hysteresis were observed in the *I*–*V* characteristics for several gold nanoparticle–molecular network ratios at higher bias voltages (up to 5 V) [6].

Dynamics during self-assembly [38] can result in structural randomness and disorder, which alter the network resistance: *I*–*V* curves measured between different electrode pairs show variations in their relative shape, and in the values of current obtained, corresponding to different paths through the network. This random variation depends on the structure and morphology of the network film formed between the electrodes, type of molecules used in the network, and on the ratio of $N_{molecule}$:$N_{particle}$, which can be used to define electronic PUFs.

To generate sequences of binary bits, electrode pair currents measured at a fixed voltage (0.5 V) were first plotted as a function of electrode pair number. For a given electrode pair, if the measured current is greater than the next pair, a value of "1" is assigned, otherwise a value of "0" is assigned. The binary bits generated in this manner can span various lengths depending on the number of electrode pairs measured for each sample and the number of current values used from each *I*–*V* curve. For example, the current profiles and corresponding 16-digit binary keys generated for gold nanoparticle–NDT networked films with N_{NDT}:$N_{particle}$ ratios of 1:1 and 50:1 are shown in Figure 2a,b, respectively.



(**a**) (**b**)

Figure 2. Current profiles measured at 0.5 V for different electrode pairs and N_{NDT}:$N_{particle}$ ratio of (**a**) 1:1 and (**b**) 50:1. Insets show the 16-bit binary key generated by comparing adjacent electrode pair currents.

Larger keys could also be obtained by combining current data for a given network ratio as shown in Figure 3a wherein the current profile generated for gold nanoparticle–NDT films with N_{NDT}:$N_{particle}$ ratio of 1:1 and control samples (no molecules) was used to produce a 128-bit stream.

Table 1. 16-bit keys produced from different self-assembled metal–molecular network sample data.

Sample Type	Key 1	Key 2	Key 3	Key 4
1:1 NDT	0111001011110001	1010110100101100	1011000101011101	1011100000010100
5:1 NDT	1010100110010010	1001001100010010	1000101100010011	1001010010101000
50:1 NDT	0101011101001011	1011000011011101	0110100110010101	0100101011001100
1:1 BDT	1000001101011000	0110101011001010	0100101010111000	1000010101101100
5:1 BDT	0100100110101001	0100010011001101	0101001001011101	0110011000010010
50:1 BDT	1010110101110110	0100101110100010	1001011001101001	0110001010101101
Control	0100101011010100	0101010100101100	0110010101101011	0110101000111100

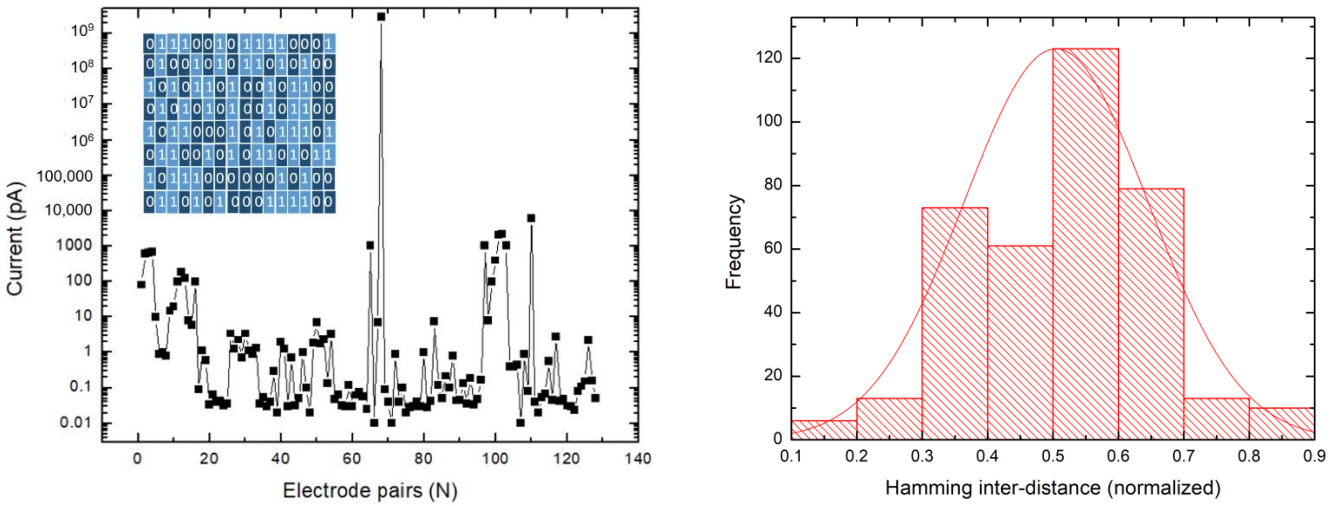


Figure 3. (**a**) Current profile built by alternately combining four 16-bit keys from gold nanoparticle–nonanedithiol networked films (1:1 ratio) with four 16-bit keys from a control sample (network without molecules). Inset shows the 128-bit key generated by comparing adjacent currents. (**b**) Histogram of normalized Hamming inter-distance for 16-bit keys shown in Table 1 using metal–molecular network sample data.

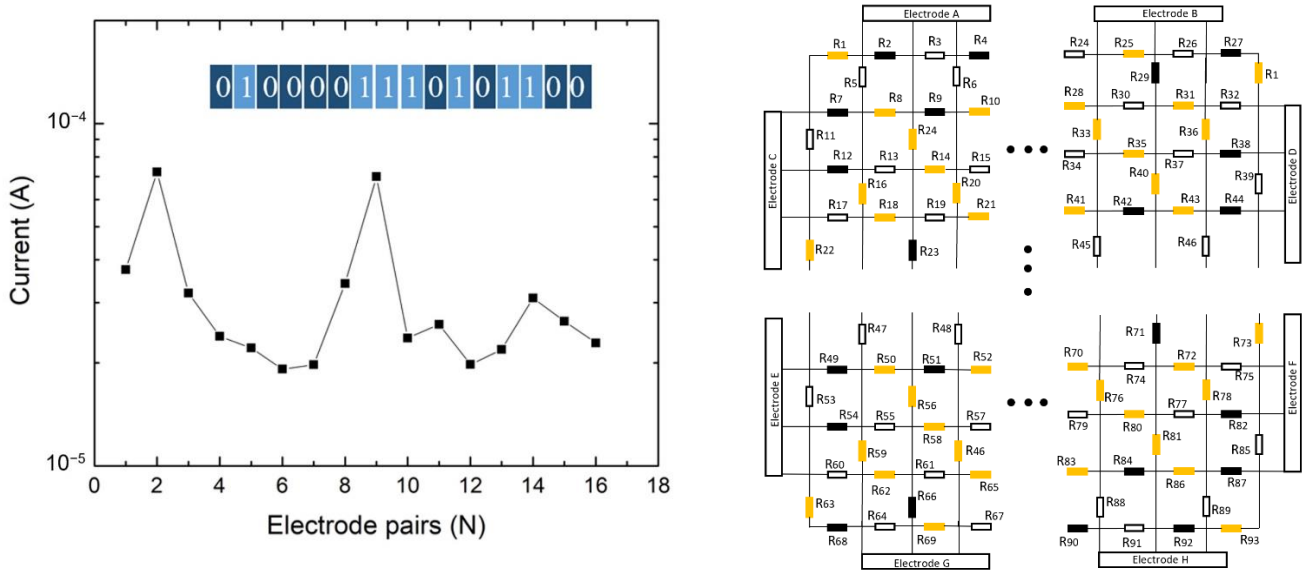
The randomness and/or uniqueness of the generated bits can be evaluated using various testing methodologies such as the NIST statistical randomness test suite [39], and the Hamming distance metric [20,40]. The Hamming distance methodology is often used to evaluate shorter keys such as those in Figure 2. By definition, the Hamming distance between two keys of equal length is the total number of changes required to make the two keys identical (typically normalized to key length), found by comparing bit-by-bit differences between keys. In our case, if the two keys are obtained from the same set of electrode pairs measured twice, we obtain the Hamming intra-distance. In contrast, the Hamming inter-distance value is obtained if the keys are from different samples. Repeated measurements from the same set of electrode pairs on our samples showed good repeatability and stability, leading to very low Hamming intra-distances. For the Hamming inter-distance, mean values near 0.5 are thought to be ideal since it implies that the two keys under consideration are random, uncorrelated, and unclonable [13]. For this study, we generated four 16-bit keys for each of the molecules and ratios shown in Table 1 corresponding to data obtained from self-assembled metal–molecular network samples and control samples without molecules.

Analysis showed the mean Hamming inter-distance varied between 0.42 to 0.53, and 0.48 to 0.6, for a given ratio NDT and BDT sample, respectively. However, if we consider all sample types with different N_{molecule}:N_{particle} network ratios in Table 1 the mean Hamming inter-distance value was very close to 0.5 (Figure 3b), which indicates that the ability to vary network composition and morphology via tunable self-assembly resulted in improved performance, and demonstrates a potential path toward implementing molecular-scale hardware security primitives using an almost continuously variable quantity, i.e., molecule-to-particle ratio (at some point, for very large ratios, the network will likely become saturated with molecules).

Longer keys were also tested for randomness using the NIST test suite: For example, the 128-bit key shown in Figure 3a passed the frequency test, frequency within a block test, cumulative sums test, cumulative sums test—reverse, and longest run of ones test with p-values > 0.01 [39]. In general, it was found that combining keys from different molecules and ratios led to an increase in the number of tests passed, but a more complete NIST

test suite analysis would generally require keys much larger than those considered in the present study.

Lastly, a linear circuit model was used to check the validity of the approach presented by utilizing a resistor network to represent the molecular network structure (see Materials and Methods). Figure 4a shows the results of low-bias circuit simulations for one such circuit simulation: The network shown in Figure 4b was probed at different locations using 8 electrodes to simulate the electrical measurements conducted on the fabricated samples. The simulated current through the molecular networks typically varied between electrode pairs and could be used to generate arrays of bits analogous to the experimental measurements.



(**a**) (**b**)

Figure 4. (**a**) 500 by 500 nm network current profile circuit simulation result for a voltage of 0.5 V applied between different electrode pairs of a molecular network with 1/3 molecular connections (roughly corresponding to a 1:1 ratio sample [30]). Inset shows the 16-bit key generated by comparing current values between adjacent electrode pairs. (**b**) 8-pad circuit configuration used for simulations.

4. Conclusions

In summary, nanoelectronic networks of colloidal gold nanoparticles interconnected with different ratios of thiolated molecules were fabricated using a tunable self-assembly process and used to create physically unclonable functions for hardware security applications. The intrinsic physical variations induced during fabrication led to electronic transport measurements on these organic–inorganic networks that displayed differences in current when probed with electrode pairs at different locations, which were utilized to generate unique arrays of binary bits for encryption keys.

By controlling the ratio of molecules to nanoparticles in the networks during self-assembly, nanoelectronic circuits with tunable morphologies allow molecular-scale hardware encryption to be realized with an additional degree of freedom for improved performance via the creation of unique security primitives that is difficult to achieve in conventional systems based on standard or "bulk" processing. The fabrication process and self-assembled electronic PUFs presented are compatible with planar silicon IC technology and packaging and can be readily scaled up for larger key generation using denser electrodes with high-resolution lithography, which may also allow them to complement existing hardware encryption systems. Future work could examine, theoretically and experimentally, the effect of non-linear electrical characteristics and hysteresis/fluctuations, defects, different molecular/nanoparticle network building blocks, network stability/possible attack vectors, and multiple-bit/non-binary key generation for hardware security applications. The low-cost solution-based fabrication approach presented shows the potential

of metal–molecular networks for improved information security via nanoscale hardware encryption primitives that create robust nanoelectronic PUFs, based on the large parameter space offered by combining different ratios of molecules and nanoparticles, with built-in redundancy and scalability.

Author Contributions: Conceptualization, C.P.; methodology, A.V., E.A. and C.P.; investigation, A.V. and E.A.; data curation, A.V. and E.A.; writing—original draft preparation, A.V. and E.A.; writing—review and editing, A.V., E.A. and C.P.; supervision, C.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Natural Sciences and Engineering Research Council of Canada and the Canada Foundation for Innovation.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thank Po Zhang for preliminary work related to the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Stan, M.R.; Franzon, P.D.; Goldstein, S.C.; Lach, J.C.; Ziegler, M.M. Molecular electronics: From devices and interconnect to circuits and architecture. *Proc. IEEE* **2003**, *91*, 1940–1957. [CrossRef]
2. Ratner, M. A brief history of molecular electronics. *Nat. Nanotechnol.* **2013**, *8*, 378–381. [CrossRef] [PubMed]
3. Amadi, E.V.; Venkataraman, A.; Zaborniak, T.; Papadopoulos, C. Nanoelectronic circuit elements based on nanoscale metal–molecular networks. *J. Comput. Electron.* **2021**, *21*, 319–333. [CrossRef]
4. Akkerman, H.B.; Blom, P.W.M.; de Leeuw, D.M.; de Boer, B. Towards molecular electronics with large-area molecular junctions. *Nature* **2006**, *441*, 69–72. [CrossRef] [PubMed]
5. Aradhya, S.V.; Venkataraman, L. Single-molecule junctions beyond electronic transport. *Nat. Nanotechnol.* **2013**, *8*, 399–410. [CrossRef] [PubMed]
6. Venkataraman, A.; Amadi, E.V.; Zaborniak, T.S.M.; Zhang, P.; Papadopoulos, C. Negative Differential Resistance and Hysteresis in Self-Assembled Nanoscale Networks with Tunable Molecule-to-Nanoparticle Ratios. *Phys. Status Solidi B* **2020**, *257*, 2000019. [CrossRef]
7. Knechtel, J. Hardware Security For and Beyond CMOS Technology: An Overview on Fundamentals, Applications, and Challenges. In Proceedings of the 2020 International Symposium on Physical Design, Taipei, Taiwan, 20–23 September 2020; 2020; pp. 75–86.
8. Smith, A.F.; Patton, P.; Skrabalak, S.E. Plasmonic Nanoparticles as a Physically Unclonable Function for Responsive Anti-Counterfeit Nanofingerprints. *Adv. Funct. Mater.* **2016**, *26*, 1315–1321. [CrossRef]
9. Gaviria Rojas, W.A.; McMorrow, J.J.; Geier, M.L.; Tang, Q.; Kim, C.H.; Marks, T.J.; Hersam, M.C. Solution-Processed Carbon Nanotube True Random Number Generator. *Nano Lett.* **2017**, *17*, 4976–4981. [CrossRef]
10. Liu, Y.; Han, F.; Li, F.; Zhao, Y.; Chen, M.; Xu, Z.; Zheng, X.; Hu, H.; Yao, J.; Guo, T.; et al. Inkjet-printed unclonable quantum dot fluorescent anti-counterfeiting labels with artificial intelligence authentication. *Nat. Commun.* **2019**, *10*, 2409. [CrossRef]
11. Rajendran, J.; Karri, R.; Wendt, J.B.; Potkonjak, M.; McDonald, N.; Rose, G.S.; Wysocki, B. Nano Meets Security: Exploring Nanoelectronic Devices for Security Applications. *Proc. IEEE* **2015**, *103*, 829–849. [CrossRef]
12. Herder, C.; Yu, M.-D.; Koushanfar, F.; Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. *Proc. IEEE* **2014**, *102*, 1126–1141. [CrossRef]
13. Halak, B. *Physically Unclonable Functions: From Basic Design Principles to Advanced Hardware Security Applications*; Springer International Publishing: Cham, Switzerland, 2018.
14. Shim, K.-A. A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 577–601. [CrossRef]
15. Katzenbeisser, S.; Kocabaş, Ü.; Rožić, V.; Sadeghi, A.-R.; Verbauwhede, I.; Wachsmann, C. PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon. In Proceedings of the Cryptographic Hardware and Embedded Systems–CHES 2012, Berlin, Germany, 9–12 September 2012; pp. 283–301.
16. Gao, Y.; Ranasinghe, D.C.; Al-Sarawi, S.F.; Kavehei, O.; Abbott, D. Emerging Physical Unclonable Functions with Nanotechnology. *IEEE Access* **2016**, *4*, 61–80. [CrossRef]
17. Rose, G.S.; Rajendran, J.; McDonald, N.; Karri, R.; Potkonjak, M.; Wysocki, B. Hardware security strategies exploiting nanoelectronic circuits. In Proceedings of the 2013 18th Asia and South Pacific Design Automation Conference (ASP-DAC), Yokohama, Japan, 22–25 January 2013; pp. 368–372.

18. Kim, J.; Yun, J.M.; Jung, J.; Song, H.; Kim, J.-B.; Ihee, H. Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires. *Nanotechnology* **2014**, *25*, 155303. [CrossRef] [PubMed]
19. Kaczmarek, A.M.; Liu, Y.-Y.; Wang, C.; Laforce, B.; Vincze, L.; Van Der Voort, P.; Van Hecke, K.; Van Deun, R. Lanthanide "Chameleon" Multistage Anti-Counterfeit Materials. *Adv. Funct. Mater.* **2017**, *27*, 1700258. [CrossRef]
20. Hu, Z.; Comeras, J.M.M.L.; Park, H.; Tang, J.; Afzali, A.; Tulevski, G.S.; Hannon, J.B.; Liehr, M.; Han, S.-J. Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. *Nat. Nanotechnol.* **2016**, *11*, 559–565. [CrossRef]
21. Moon, D.-I.; Rukhin, A.; Gandhiraman, R.P.; Kim, B.; Kim, S.; Seol, M.-L.; Yoon, K.J.; Lee, D.; Koehne, J.; Han, J.-W.; et al. Physically Unclonable Function by an All-Printed Carbon Nanotube Network. *ACS Appl. Electron. Mater.* **2019**, *1*, 1162–1168. [CrossRef]
22. Burzurí, E.; Granados, D.; Pérez, E.M. Physically Unclonable Functions Based on Single-Walled Carbon Nanotubes: A Scalable and Inexpensive Method toward Unique Identifiers. *ACS Appl. Nano Mater.* **2019**, *2*, 1796–1801. [CrossRef]
23. Hwang, K.-M.; Park, J.-Y.; Bae, H.; Lee, S.-W.; Kim, C.-K.; Seo, M.; Im, H.; Kim, D.-H.; Kim, S.-Y.; Lee, G.-B.; et al. Nano-electromechanical Switch Based on a Physical Unclonable Function for Highly Robust and Stable Performance in Harsh Environments. *ACS Nano* **2017**, *11*, 12547–12552. [CrossRef]
24. Jiang, H.; Belkin, D.; Savel'ev, S.E.; Lin, S.; Wang, Z.; Li, Y.; Joshi, S.; Midya, R.; Li, C.; Rao, M.; et al. A novel true random number generator based on a stochastic diffusive memristor. *Nat. Commun.* **2017**, *8*, 882. [CrossRef]
25. Zhang, T.; Guérin, D.; Alibart, F.; Vuillaume, D.; Lmimouni, K.; Lenfant, S.; Yassin, A.; Oçafrain, M.; Blanchard, P.; Roncali, J. Negative Differential Resistance, Memory, and Reconfigurable Logic Functions Based on Monolayer Devices Derived from Gold Nanoparticles Functionalized with Electropolymerizable TEDOT Units. *J. Phys. Chem. C* **2017**, *121*, 10131–10139. [CrossRef]
26. Nijhuis, C.A.; Reus, W.F.; Barber, J.R.; Dickey, M.D.; Whitesides, G.M. Charge Transport and Rectification in Arrays of SAM-Based Tunneling Junctions. *Nano Lett.* **2010**, *10*, 3611–3619. [CrossRef] [PubMed]
27. Zheng, J.; Zhang, J.; Wang, Z.; Zhong, L.; Sun, Y.; Liang, Z.; Li, Y.; Jiang, L.; Chen, X.; Chi, L. Programmable Negative Differential Resistance Effects Based on Self-Assembled Au@PPy Core–Shell Nanoparticle Arrays. *Adv. Mater.* **2018**, *30*, 1802731. [CrossRef] [PubMed]
28. Dadosh, T.; Gordin, Y.; Krahne, R.; Khivrich, I.; Mahalu, D.; Frydman, V.; Sperling, J.; Yacoby, A.; Bar, J. Measurement of the conductance of single conjugated molecules. *Nature* **2005**, *436*, 1200–1200. [CrossRef]
29. Weisbecker, C.S.; Merritt, M.V.; Whitesides, G.M. Molecular Self-Assembly of Aliphatic Thiols on Gold Colloids. *Langmuir* **1996**, *12*, 3763–3772. [CrossRef]
30. Zhang, P.; Venkataraman, A.; Papadopoulos, C. Self-assembled gold nanoparticle-molecular electronic networks: Self-assembled gold nanoparticle-molecular networks. *Phys. Status Solidi B* **2017**, *254*, 1700061. [CrossRef]
31. Mozharov, A.M.; Vasiliev, A.A.; Bolshakov, A.D.; Sapunov, G.A.; Fedorov, V.V.; Cirlin, G.E.; Mukhin, I.S. Core-Shell III-Nitride Nanowire Heterostructure: Negative Differential Resistance and Device Application Potential. *Semiconductors* **2018**, *52*, 489–492. [CrossRef]
32. Bruot, C.; Hihath, J.; Tao, N. Mechanically controlled molecular orbital alignment in single molecule junctions. *Nat. Nanotechnol.* **2011**, *7*, 35–40. [CrossRef]
33. Kockmann, D.; Poelsema, B.; Zandvliet, H.J.W. Transport through a Single Octanethiol Molecule. *Nano Lett.* **2009**, *9*, 1147–1151. [CrossRef]
34. Xu, B.; Tao, N.J. Measurement of Single-Molecule Resistance by Repeated Formation of Molecular Junctions. *Sci. (Am. Assoc. Adv. Sci.* **2003**, *301*, 1221–1223. [CrossRef]
35. Chu, C.; Na, J.-S.; Parsons, G.N. Conductivity in Alkylamine/Gold and Alkanethiol/Gold Molecular Junctions Measured in Molecule/Nanoparticle/Molecule Bridges and Conducting Probe Structures. *J. Am. Chem. Soc.* **2007**, *129*, 2287–2296. [CrossRef] [PubMed]
36. Wold, D.J.; Frisbie, C.D. Fabrication and Characterization of Metal−Molecule−Metal Junctions by Conducting Probe Atomic Force Microscopy. *J. Am. Chem. Soc.* **2001**, *123*, 5549–5556. [CrossRef] [PubMed]
37. Engelkes, V.B.; Beebe, J.M.; Frisbie, C.D. Length-Dependent Transport in Molecular Junctions Based on SAMs of Alkanethiols and Alkanedithiols: Effect of Metal Work Function and Applied Bias on Tunneling Efficiency and Contact Resistance. *J. Am. Chem. Soc.* **2004**, *126*, 14287–14296. [CrossRef] [PubMed]
38. Amadi, E.V.; Venkataraman, A.; Papadopoulos, C. Nanoscale self-assembly: Concepts, applications and challenges. *Nanotechnology* **2022**, *33*, 132001. [CrossRef] [PubMed]
39. Rukhin, A.L.; Soto, J.; Nechvatal, J.R.; Smid, M.E.; Barker, E.B.; Leigh, S.D.; Levenson, M.; Vangel, M.; Banks, D.L. Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications. 2010. Available online: https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final (accessed on 15 May 2022).
40. Waggener, W.N. *Pulse Code Modulation Techniques: With Applications in Communications and Data Recording*; Van Nostrand Reinhold: New York, NY, USA, 1995.