Nanotechnology-Based Trusted Remote Sensing

James B. Wendt and Miodrag Potkonjak
Computer Science Department
University of California, Los Angeles
{jwendt, miodrag}@cs.ucla.edu

Abstract—**We present a new nanotechnology PPUF-based architecture for trusted remote sensing. Current public physical unclonable function designs encompass complex circuits requiring high measurement accuracy and whose size slows down the authentication process. Our novel nanotechnology-based architecture ensures fast authentication through partial simulation while maintaining robust security. We authenticate over partitions in the design space in order to alleviate the authentication burden while still ensuring attack by simulation is entirely ineffective. We contribute new nanotechnology-based security protocols for authentication and time-stamping for trusted remote sensing.**

I. INTRODUCTION

Trust is an essential component in communication systems and applications ranging from social networks to e-commerce to remote sensing. With the advancement of mobile devices and embedded sensing it is imperative that trust become a top design consideration. Without trusted remote sensing, an attacker could replace an office security camera with a blank tape recording of the room while a burglar freely roams about. To prevent this intrusive switch from successfully tricking our security center, incorporating a secure authentication system between the remote sensor (the security camera) and the authenticator (the security center receiving the camera feed) will ensure that the receiving feed is in fact being delivered from the original untampered device.

Numerous metrics are considered when designing sensor systems including accuracy, lifetime, power demands, and costs. Power usage is a major concern for many remote sensor networks that are battery operated and far removed from accessibility. For the security component of the remote sensor, it is essential that the authentication speed be ultra fast to ensure that an attacker cannot react quickly enough to stolen network requests to produce a believable response in a reasonable amount of time.

Current solutions to ensure trusted remote sensing utilize physical unclonable functions (PUFs) and their counterparts, public physical unclonable functions (PPUFs), to execute authentication protocols between remote sensors and an authenticating party [1]. PUFs are physical systems with multiple inputs producing corresponding outputs that are difficult to predict or calculate. The design and physical characteristics inherent in the PUF also make it exceedingly difficult to reverse engineer or reproduce. PPUFs are PUFs that are intentionally made easy to reverse engineer such that the extracted parameters of the physical system serve as the device's public key and the system's input-output mapping as the device's secret key. While the full characterization of the PPUF is made public, cloning or simulation of that characterization in order to recreate or predict its input-output mappings remains infeasible. The key observation is that only the owner of the PPUF can easily and rapidly compute the output (response) for a given input (challenge), while anyone with the complete characterization of the PPUF can confirm a response was mapped from an original challenge.

Authentication of current CMOS-based PPUFs is achieved through full device simulation. Unfortunately, the size and complexity of the design is coupled to both the security and authentication time of the device. Larger and more complex devices provide stronger security, but also longer authentication times. Traditional CMOS-based PPUF designs also require high accuracy measurements utilizing high frequency clocks and high resolution timing [2].

In this paper we propose the use of nanotechnology for the creation of PPUFs and their application to trusted remote sensing. Many potential nanotechnologies promise to be faster, smaller, and demand less power than their semiconductor counterparts. Additionally, the random synthesis methods with which many nanotechnology devices are fashioned generate impossible to clone components.

By capitalizing on the analog nature of these new nanotechnology devices we are able to eradicate the need for high resolution measurements and exceedingly long authentication times while still retaining robust security. We use as our driving example, the nanocell, and show that our authentication and time-stamping protocols require only partial simulation of the nanocell-based PPUF.

II. RELATED RESEARCH

A. *Physical Unlonable Function*

Born out of the original optical physically one-way function [3], PUFs have been realized in integrated circuits and applied to security applications ranging from ID creation and authentication to hardware metering, and remote system control [4] [5] [6] [7].

One of the first integrated circuit PUFs, the delay-based silicon PUF, leverages the intrinsic process variation of submicron technologies in order to be unique and unclonable [4]. However, the original implementation of a silicon-based PUF is limited to only secret key cryptography and authentication through the use of lookup tables of input-output (challenge-response) pairs.

978-1-4244-9289-3/11/$26.00 ©2011 IEEE

B. *Public Physical Unclonable Function*

The PPUF improves upon the PUF by introducing the more common public key cryptographic protocols. *Beckmann, et. al.* [2] proposed a model for the first PPUF with accompanying protocols for public key cryptographic communication and secure secret key exchange by utilizing gate-level characteristics, such as leakage energy and delay, to represent the PPUF public key. However, this approach requires high frequency clocks, high resolution timing, and long simulation times for authentication.

Even recent solutions using low power, high speed PPUFs still require full simulation for authentication [1] [8] and are much too long for remote sensing applications. By leveraging the effects of device aging, two CMOS-based PPUFs can be matched to one another such that their challenge-response pairs become identical [9] [10], ultimately removing the need for simulation in authentication altogether. Unfortunately, this comes at the cost of device aging and requires very high resolution measurements.

C. *Nanotechnology*

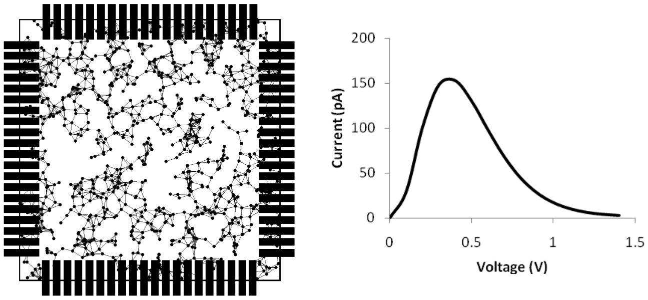
The development of nanotechnology research continues to lead to advances in medical science and material science, and has recently spread into computer engineering and electrical engineering. Current trends in nanotechnology-based computing focus on synthesizing molecular electronic devices in an attempt to obtain systematic results from disorderly chemical processes. *Dick, et. al.* [11] demonstrate promising results controlling the production of three-dimensional networks of Indium Arsenide (InAs) nanowires that display non-linear current-voltage (I-V) characteristics that could be harnessed in molecular electronic logic devices [11] [12]. However, the self-assembled nature of these networks remains innately random. For application of this nanotechnology (and others like it) to PUFs, this randomness is desirable.

Our report is the first that we know of to apply nanotechnology to PUFs and PPUFs in small form embedded systems for trusted remote sensing.

D. *Cryptographic Protocols*

Public key encryption algorithms such as RSA have been utilized to safeguard privacy when communicating over unsecure networks [13] [14] [15] [16] [17] [18] [19]. There has been a significant amount of work in numerous reputation schemes [20] [21] [22] [23] [24] [25] which are geared most towards applications in WWW, peer-to-peer networks, data filtering and social networks [26] [27] [28] [29] [30] [31].

Our new nanotechnology-based trusted remote sensing system relies partly on the notion of administering random challenges which many cryptographic methods and security procedures depend upon as well [15] [32] [33] [34] [35] [36]. Furthermore, we are able to introduce another degree of unpredictability by utilizing the large input space of our nanotechnology architecture. Specifically, pins are not statically assigned as inputs or outputs at design time, but rather can be chosen to be either inputs or outputs once a challenge is administered.



(a) (b)

Figure 1: (a) Example of a 2μm × 2μm nanocell containing about 1000 nanoparticles with an average degree of 6. The black rectangles represent the 80 input/output pins. (b) I-V characteristics of a single monolayer

III. Preliminaries

A. *Nanocell*

In this paper, our target nanotechnology is the nanocell, effectively a non-linear two-dimensional network of randomly distributed metallic particles connected by self-assembled molecules, called monolayers, that exhibit I-V characteristics with negative differential resistance (NDR) [37] [38] [39]. Other similar nanotechnologies, such as the InAs nanowires also posses similar non-linear and network-like characteristics; however they have not been studied in the same capacity as the nanocell.

Using the nanocell as a PPUF is possible in part due to the non-linearity of the I-V curve of the monolayers that connect its network. For simplicity in simulation and convergence using the SPICE circuit simulator, we use the approximate curve shown in Figure 1b derived from [37] [40] [41] to represent a single monolayer's I-V characteristics. The non-linearity in this curve along with the random placement of nodes and random assembly of monolayers helps form the non-linear challenge-response mappings for the nanocell-based PPUF.

B. *Circuit Simulation*

The monolayers and nanoparticles constituting the nanocell network can be simulated as non-linear elements and node connections, respectively, in an electronic circuit. This complicated circuit can be simplified to a system of equations defined by Kirchoff's Current and Voltage laws. In order to solve this large system of equations we utilize the node voltage analysis capabilities of the SPICE circuit simulator.

IV. Nanocell PPUF

A. *Simulation*

For the purposes of simulating the nanocell as a PPUF, we distribute one thousand nodes uniformly and randomly across a 2μm × 2μm silicon wafer and draw an edge between nodes that fall within a threshold distance of 45nm, which yields an average degree of about 5.5 to 6.3. The density of nodes and density of monolayers is similar to the observations in [37]. We also ensure that the network is fully connected to ensure node voltage analysis convergence by the SPICE simulator.

The physical locations of twenty equally spaced pin positions along each edge, protruding 0.3μm into the nanocell,

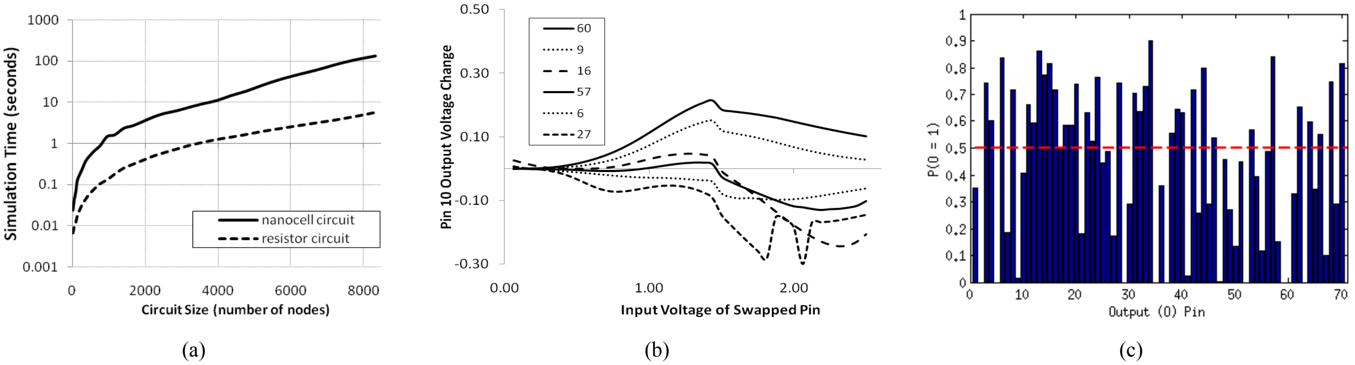


Figure 2: (a) SPICE simulation time for the nanocell and equivalent linear circuit network. (b) Nine pins of a nanocell are set as static inputs and a tenth input is swapped from Pin 1 to Pin *X* (denoted in legend). The resulting chaotic output at pin 10 is graphed. (c) Likelihood of output pin O_i being 1 for the nanocell PPUF described. The red dashed line depicts the ideal case, where $P(O_i = 1) = 0.5$ for all output pins.

are calculated. For SPICE simulation, those nodes that are engulfed by a pin are short-circuited to that pin in the SPICE netlist.

The monolayers (NDR circuit devices) between nanoparticles (nodes) are simulated using the approximated I-V curve in Figure 1b. Before simulation, a set of pins is assigned as inputs and applied various voltages at which point we instruct the SPICE circuit simulator to perform a node voltage analysis on the constructed circuit.

B. *Partitioning*

Current CMOS-based PPUF designs require full simulation in order to authenticate challenge-response pairs. While a smaller design would be easier to authenticate, it would also be much less secure. These conflicting requirements prevent the CMOS-based PPUF design from scaling.

On the other hand, the analog nature of the nanocell allows for the device to grow to an arbitrary size while maintaining a constant and practical authentication time. This is accomplished by dividing the network into partitions and authenticating the challenge-response pair over only one or a few of the partitions. The nanocell remains a connected network, while arbitrary lines are drawn throughout to partition the space.

An attacker does not know which set of partitions the authenticating party will test, thus he must simulate the entire nanocell in order to attempt an attack.

C. *Input Space*

Unique to nanocells that has not yet been realized in CMOS-based PUFs is the ability to not only dynamically choose input values, but to also dynamically choose input pins. As with the majority of integrated circuits, CMOS-based PUFs are one-way devices that have statically assigned input pins on which only the input values can vary. Utilizing the nanocell as an analog device offers the freedom to dynamically choose input pins each time a challenge is administered, effectively increasing the input space exponentially with the number of pins.

V. SIMULATION RESULTS

A. *Scalability & Resistance to Simulation Attacks*

As both linear and non-linear circuit size increase, simulation time grows exponentially and grows an order of magnitude faster for non-linear circuits than for linear. A nanocell-based PPUF with millions of nodes will be prohibitively expensive to fully simulate. This expensive simulation cost coupled with the aforementioned partitioning scheme allows for the nanocell PPUF to scale larger, ultimately becoming impervious to attack by simulation, while maintaining that authentication remains quick and secure.

B. *Resiliency Against Statistical Attacks*

Statistical guessing is another plausible attack that could befall our device. The easiest to address is random guessing. This method is most infeasible due to the number of input/output pins we can place on our nanocell. Figure 2c illustrates for the probability of randomly guessing each of the output pins.

A more genuine attack might be one grounded in advanced statistics than random guessing. The nanocell-based PPUF is safe against these attacks due to its large and malleable input space. For a single nanocell there exists 2^{80} possible input sets, each defining a very non-linear and unique challenge-response mapping. Even if the mappings could be predicted it is impossible to construct 2^{80} statistical models representing each input set.

In Figure 2b we show by making the smallest change to the input set that is possible (switching a single input pin with an output pin) that there is a dramatic and unpredictable change in output over varying inputs values.

VI. TRUSTED REMOTE AUTHENTICATION

The following authentication protocol enables the authenticating party (AP) to trustfully request and receive data from a remote sensor. The AP sends to the remote sensor a challenge, *C*. The sensor applies two challenges to its PPUF, $C \rightarrow R$ and $C \veebar S \rightarrow R'$, where *S* is the signal to be sent and *R* and *R'* are the responses. The signal *S* is XORed with the challenge at each allocated partition of the nanocell-based PPUF. This enables the AP to extract the signal in a timely fashion by simulating over only one of the partitions. After computing R and R', the sensor sends both responses to the AP. The AP confirms via simulation over a small partition of the PPUF that R is the correct response to C, and subsequently computes $R' \veebar C \rightarrow S$. To ensure that S is genuine, the AP also checks that R' is the correct response to $C \veebar S$ via simulation.

Time-stamping is achieved in real-time by receiving a response from the remote sensor immediately after a challenge is administered. Since simulation of a full nanocell-based PPUF is impossible to complete in a timely fashion, a quick and correct response can only mean that we received a correct timestamp from the trusted remote sensor.

VII. Conclusion

In this paper we presented a new nanotechnology PPUF-based architecture for trusted remote sensing illustrated using the nanocell. Nanotechnology promises to be faster and use less power than conventional CMOS technology. We have also shown that it scales better for security.

We have introduced a new nanotechnology PPUF-based secure cryptographic protocol and have shown that it requires only partial simulation of the nanoPPUF for authentication while still maintaining that attack by simulation or statistical guessing is impossible.

References

[1] M. Potkonjak, S. Meguerdichian, and J. L. Wong, "Trusted sensors and remote sensing," IEEE Sensors, pp. 1104-1107, 2010.

[2] N. Beckmann and M. Potkonjak, "Hardware-based public-key cryptography with public physically unclonable functions," Info. Hiding, pp. 206-220, 2009.

[3] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," Science, vol. 297, no. 5589, pp. 170-178, 2002.

[4] B. Gassend, D. Clarke, M. Van Dijk and S. Devadas, "Silicon physical random functions," Proc. of the Conference on CCS, pp 148-160, 2002

[5] S. Trimberger, "Trusted design in FPGAs," Proc. of the 44th DAC, pp. 5-8, 2007.

[6] F. Koushanfar and M. Potkonjak, "CAD-based security, cryptography, and digital rights management," Proc. of the 44th DAC, pp. 268-269, 2007.

[7] Y. M. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," Proc. of the USENIX Sec. Symp., pp. 1-16, 2007.

[8] M. Potkonjak, S. Meguerdichian, A. Nahapetian, and S. Wei, "Differential public physically unclonable functions: architecture and applications," Proc. of the 48th DAC, 2011.

[9] S. Meguerdichian and M. Potkonjak, "Device aging-based physically unclonable functions," Proc. of the 48th DAC, 2011.

[10] S. Meguerdichian and M. Potkonjak, "Matched public PUF: ultra low energy security platform," Intl. Symp. on Low Power Electronic Devices, 2011.

[11] K. A. Dick, K. Deppert, L. S. Karlsson, W. Seifert, L. R. Wallenberg, and L. Samuelson, "Position-controlled interconnected InAs nanowire networks," Nano Lett., vol. 6, pp. 2842-2847, 2006.

[12] L.-E. Wernersson, C. Thelander, E. Lind, and L. Samuelson, "III-V nanowires—extending a narrowing road," Proc of the IEEE, vol. 98, no. 12, pp. 2047-2060, 2010.

[13] I. Blake, G. Seroussi, and N. Smart, Elliptic Curves in Cryptography, Cambridge Univ Pr, 1999.

[14] D. Boneh and H. Shacham, "Fast variants of RSA," Cryptobytes (RSA Laboratories), pp 1-8, 2002.

[15] W. Diffie and M. Hellman, "New directions in cryptography," TIT, vol. 22, no. 6, pp. 644-654, 1976.

[16] J. Fry and M. Langhammer, "RSA and public key cryptography in FPGAs," Tech. Report TR CF-032305-1.0, Altera Corporation, 2005.

[17] N. Gura, et al., "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," CHES, pp. 119-132, 2004.

[18] D. Hankerson, S. Vanstone, and A. Menezes, Guide to Elliptic Curve Cryptography, Springer-Verlag New York Inc., 2004.

[19] K. Paterson, "ID-based signatures from pairings on elliptic curves," Electronics Letters, vol. 38, no. 18, pp. 1025-1026, 2002.

[20] S. Buchegger and J. Le Boudec, "A robust reputation system for mobile ad-hoc networks," P2PEcon, 2004.

[21] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," DSS, vol. 43, no. 2, pp. 618-644, 2007.

[22] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," WWW, pp. 640-651, 2003.

[23] M. Nowak and K. Sigmund, "Evolution of indirect reciprocity," Nature, vol. 437, no. 7063, pp. 1291-1298, 2005.

[24] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," CACM, vol. 43, no. 12, pp. 45-48, 2000.

[25] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBays reputation system," Advances in Applied Microeconomics, vol. 11, pp. 127-157, 2002.

[26] L. Adamic and E. Adar, "How to search a social network," Social Networks, vol. 27, no. 3, pp. 187-203, 2005.

[27] S. Androutsellis-Theotokis and D. Spinellis, "A survey of peer-to-peer content distribution technologies," CSUR, vol. 36, no. 4, p. 371, 2004.

[28] J. Kleinberg, "The convergence of social and technological networks," CACM, vol. 51, no. 11, pp. 66-72, 2008.

[29] R. Kumar, J. Novak, and A. Tomkins, "Structure and evolution of online social networks," SIGKDD, p. 617, 2006.

[30] D. Liben-Nowell, J. Novak, R. Kumar, P. Raghavan, and A. Tomkins, "Geographic routing in social networks," PNAS, vol. 102, no. 33, page. 11623, 2005.

[31] B. Zhou and J. Pei, "Preserving privacy in social networks against neighborhood attacks," ICDE, pp. 506-515, 2008.

[32] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley Publishing, 2008.

[33] R. Anderson and M. Kuhn, "Tamper resistance: a cautionary note," USENIX EC, vol. 2, p. 1, 1996

[34] A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[35] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, A1bazaar, 2007.

[36] F. Stajano, "The resurrecting duckling," Security Protocols, pp. 215-222, 2000.

[37] J. M. Tour, W. L. VanZandt, C. P. Husband, S. M. Husband, L. S. Wilson, P. D. Franzon and D. P. Nackashi, "NanoCell logic gates for molecular computing," IEEE Trans. Nanotechnol., vol. 1, pp. 100, 2002.

[38] C. P. Husband, S. M. Husband, J. S. Daniels and J. M. Tour, "Logic and memory with nanocell circuits," IEEE Trans. Electron Devices, vol. 50, pp. 1865, 2003.

[39] J. M. Tour, L. Cheng, D. P. Nackashi, Y. Yao, A. K. Flatt, S. K. S. Angelo, T. E. Mallouk, and P. D. Franzon, "Nanocell electronic memories," J. Amer. Chem. Soc., vol. 125, no. 43, pp. 13279-13283, 2003.

[40] J. Chen, W. Wang, M. A. Reed, A. M. Rawlett, D. W. Price, and J. M. Tour, "Room-temperature negative differential resistance in nanoscale molecular junctions," Appl. Phys, Lett., vol. 77, pp. 1224-1226, 2000.

[41] J. Chen, M. A. Reed, A. M. Rawlett, and J. M. Tour, "Large on-off ratios and negative differential resistance in a molecular electronic device," Science, vol. 286, pp. 1550-1552, 1999.