Deterministic Tagging Technology for Device Authentication

Jungjoon Ahn
Semiconductor and Dimensional Metrology Division, Physical Measurement Laboratory
National Institute of Standards and Technology (NIST)
Gaithersburg, MD US
Jungjoon.ahn@nist.gov

Jihong Kim
Department of Electrical Engineering
Yeungnam University
Gyeongsan, Republic of Korea
jihongkim@yu.ac.kr

Joseph J. Kopanski
Semiconductor and Dimensional Metrology Division, Physical Measurement Laboratory
National Institute of Standards and Technology (NIST)
Gaithersburg, MD US
joseph.kopanski@nist.gov

Yaw S. Obeng
Semiconductor and Dimensional Metrology Division, Physical Measurement Laboratory
National Institute of Standards and Technology (NIST)
Gaithersburg, MD US
yaw.obeng@nist.gov

***Abstract*—This paper discusses the development of a rapid, large-scale integration of deterministic dopant placement technique for encoding information in physical structures at the nanoscale. The doped structures bestow a customizable radiofrequency (RF) electronic signature, which could be leveraged into a distinctive identification tag. This will allow any manufactured item (integrated circuit, pharmaceutical, etc.) to be uniquely authenticatable. Applications of this technology include enabling a secure Internet of Things (IoT) and eliminating counterfeit products.**

Keywords—Nanoelectronics, reliability, metrology, system security, probe assisted deterministic doping, PAD

I. Introduction

The Internet of Things (IoT) represents a new era of telecommunications made possible by the reduced cost of performance in electronic devices, the convergence of wireless technologies, advancements of analog systems (e.g., MEMS) and digital electronics (i.e. More-than-Moore technologies). How these devices connect to each other, and to humans, are changing how we work and live. Unfortunately, the weaknesses of the underlying networks have been exposed through the exploitation of hardware operation weaknesses. Without ample security measures, the ever-expanding sensor network could create massive vulnerabilities [1-2]. Hardware security based on a dynamic electronic tagging system that supports unique and encrypted identification is a prerequisite component of the security envelope.

The ability to tag an item by deterministically placing small clusters of dopants at the nanoscale reveals some interesting possibilities for device fabrication [3]. One promising application is the selective placement of dopants to tune the electrical properties of nano-channel MOSFETs [4-7]. Another possibility is the implantation of dopant clusters to modify the barrier height in metal-semiconductor junctions.

The probe assisted doping technique (PAD) provides the ability to rapidly produce customizable 2D-superlattices of p-n junctions on a semiconductor substrate by controlling the dopant concentration of each element (Fig. 1.) [8].

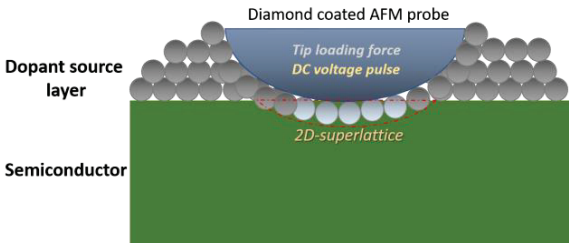

Fig. 1. Schematic representation of PAD.

PAD uses the tip-loading force and bias pulse of the probe in scanning probe microscopy (SPM) to achieve precise area control and subsequent verification imaging to implant dopants from a thin over-layer of source material. In contrast to other deterministic doping techniques, relatively large (20 x 20) 2-D superlattices can be readily formed with minimal impact to the semiconductor surface. The other advantages of PAD include (i) multiple patterns of doped semiconductor without photolithography and (ii) highly selective doping as compared to traditional invasive ion-implantation processes. While other deterministic doping processes (e.g., laser-enhance deposition and the single-ion on-demand technique) may have some advantages, they are more complex and require significant equipment investment [9]. The degrees of freedom in design and fabrication of PAD promotes a new class of low-cost identification tags for complex integrated semiconductor devices. Since photo-lithography process are not involved, each element of the array can be uniquely programmed with different structures and elemental configuration.

As an initial demonstration, clusters of aluminum (Al) atoms were deterministically doped into a wafer of n-type Si (100) to generate nanoscale counter-doped junctions within a

978-1-6654-4998-4/21/$31.00 ©2021 IEEE

few nanometers from Si-air interface. The resulting local electrical potential changes, reported as the contact potential difference (CPD), were verified with a scanning Kelvin probe microscope (SKPM). The electrical activation of nanojunctions was achieved after thermal annealing. Thermal activation, however, also promoted the diffusion of the dopants that results in an expansion of the deterministically doped sites [8].

II. EXPERIMENTAL

We adopted and modified the nano-indentation mode of the atomic force microscopy (AFM). A diamond coated tip (tip radius ~ 50 nm) on a stiff cantilever (spring constant ~ 60 N/m) rapidly created a 20 x 20 array of Al-injected p-n junctions over a 10 µm x 10 µm area of n-type Si substrates (1 Ω·cm to 10 Ω·cm). A thin Al dopant layer of 10 nm was deposited over the Si substrates using e-beam evaporator. The modified nano-indentation of each doping site was conducted by applying (i) identical trigger-threshold voltages (i.e., tip loading force) between 6 V to 8 V and (ii) a voltage pulse of 8 V that were adopted from the previously PAD experiments [8]. The x-y radius of each resulting injection site varied from 65 nm to 100 nm.

After PAD, the Al layer was chemically removed using a selective etchant. The resulting Si substrate was annealed for 30 sec that lead to diffusion of Al dopants and an activation. For post-PAD process measurements, we used scanning Kelvin force microscopy (SKFM) to measure the surface potential between the tip coating and the surface.

III. RESULTS AND APPLICATIONS

We used PAD to create arrays of Al-Si junctions as a potential nanoscale equivalent to the two-dimensional Quick Response (QR) code.

Fig. 2 shows the resulting surface potential difference after PAD of Al into the Si substrate. The potential differences varied from -10 mV to -50 mV as compared to undoped areas of the Si substrate. The greater potential differences correlated with the tip loading force gradually increased from 6 V in the bottom row to 8V in the top row of Fig. 2. Post-PAD measurements are not limited to SKFM and could employ

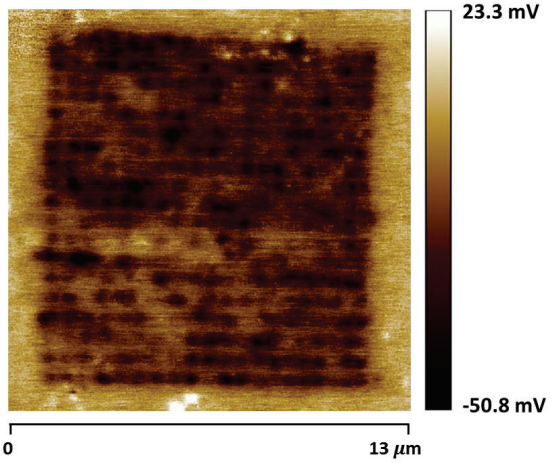

Fig. 2. SKFM image Al dopants injected and activated n-Si surface via PAD. A platinum (Pt) coated tip was used for SKFM

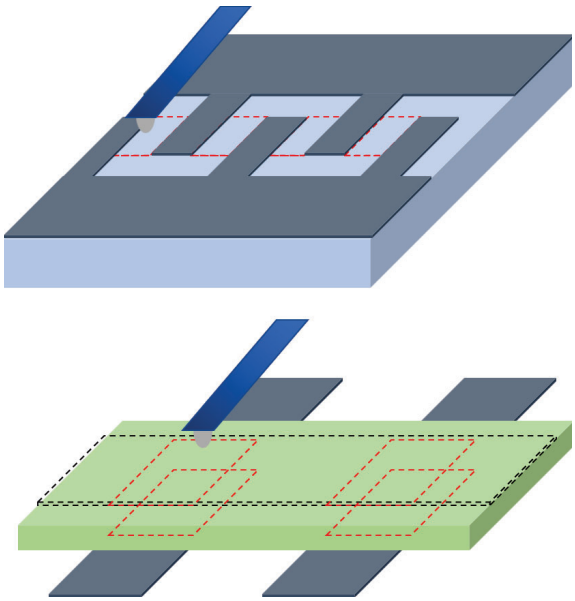

Fig. 3. Schematic representation of PAD for the device application (red dashed line). (Top) Semiconductor channel. (Bottom) Metal/semiconductor interface.

other scanning probe microscopy techniques, such as capacitance measurements with scanning microwave microscope (SMM).

In theory, the modified surface potential changes should be directly dependent on the changes in the local crystallographic structure of the Si substrate [10] and the presence of dopants. However, we noticed some inconsistencies in the surface potential differences between areas doped under the same tip loading force, which we attributed to the non-uniformities in the Al overlayer.

The PAD arrays embedded within the silicon substrate have minimal topographic impact, which allows for direct processing on semiconductor layers or within layers deposited specifically for this process, such as a thin organic semiconductor or metal layer (Fig. 3). Unlike other substrate modifying techniques, such as through silicon visa (TSV), PAD is not expected to alter the stress in the substrate nor impact device performance [11]. Furthermore, the substrate doping technique is not limited by device geometry or dimensions [12].

PAD has the potential of storing large amounts of dense data with extensive encryption and sophisticated error correction algorithms. While optically readable codes have two levels (black and white), electromagnetic codes conceivably could have multiple levels of charge, potential, or magnetic moments to expand the data density beyond the simple bit. Arrays of such information could become an intrinsic, un-removable, un-alterable, un-forgeable and encrypted part of an integrated circuit. Thus, we propose PAD as a device tagging technique to enable tamper-proof authentication certificates for devices on the internet [13-14].

IV. CONCLUSIONS AND FUTURE WORK

The ideal tag would be rapid and cheap to apply and read, un-removable, un-alterable, un-forgeable and encrypted. Our proposed new taggant system, via PAD, could meet these criteria with minimal operational cost. Each system would contain an intrinsic electronic component, traceable to the manufacturer and readable at any inspection point. The PAD technique is flexible enough to accommodate application specific customization. Future work will entail the optimization and automation of massively parallel deterministic doping [15], selection of suitable electromagnetic (EM) active dopants with high-reporting cross-sections and the development of the appropriate EM detectors/sensors.

REFERENCES

[1] Y. S. Obeng, C. Nolan and D. Brown, "Hardware security through chain assurance," 2016 Design, Automation & Test in Europe Conference & Exhibition, pp. 1535-1537, 2016.

[2] Y. S. Obeng, "Hardware Security to Mitigate Threats to Networked More-Than-Moore Sensors", 2016 ECS Trans., vol. 72, pp. 113, 2016.

[3] M. Hori, T. Shinada, Y. Ono, A. Komatsubara, K. Kumagai, T. Tanii, et al., "Impact of a few dopant positions controlled by deterministic single-ion doping on the transconductance of field-effect transistors," Applied Physics Letters, vol. 99, p. 062103, 2011

[4] J. Meijer, T. Vogel, B. Burchard, I. W. Rangelow, L. Bischoff, J. Wrachtrup, *et al.*, "Concept of deterministic single ion doping with sub-nm spatial resolution," Applied Physics A, vol. 83, pp. 321-327, 2006.

[5] R. W. Keyes, "Physical limits of silicon transistors and circuits," Reports on Progress in Physics, vol. 68, p. 2701, 2005.

[6] T. Shinada, S. Okamoto, T. Kobayashi, and I. Ohdomari, "Enhancing semiconductor device performance using ordered dopant arrays," Nature, vol. 437, pp. 1128-1131, 2005.

[7] H. Sellier, G. P. Lansbergen, J. Caro, S. Rogge, N. Collaert, I. Ferain, *et al.*, "Transport Spectroscopy of a Single Dopant in a Gated Silicon Nanowire," Physical Review Letters, vol. 97, p. 206805, 2006.

[8] J. -J. Ahn, S. D. Solares, L. You, H. Noh, J. Kopanski, and Y. Obeng , "Probe assisted localized doping of aluminum into silicon substrates", Journal of Applied Physics vol. 125, 075706, 2019.

[9] E. Prati and T. Shinada, Single-Atom Nanoelectronics, Pan Stanford Publishing, 2013.

[10] K. Mylvaganam, L. C. Zhang, P. Eyben, J. Mody, and W. Vandervorst, "Evolution of metastable phases in silicon during nanoindentation: mechanism analysis and experimental verification", Nanotechnology, vol. 20, 305705, pp. 8, 2009 .

[11] Athikulwongse, K., et al. *Stress-driven 3D-IC placement with TSV keep-out zone and regularity study*. in *2010 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. 2010.

[12] Ieong, M., et al., *Silicon Device Scaling to the Sub-10-nm Regime.* Science, 2004. **306**(5704): p. 2057-2060.

[13] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, vol. 11, pp. 2710-2723, 2013.

[14] Y.S. Obeng, J. J. Kopanski, J.-J. Ahn, "Authentication article and process for making same, Patent number: US 10152666

[15] Vettiger, P., et al., *The "millipede" - nanotechnology entering data storage.* IEEE Transactions on Nanotechnology, 2002. **1**(1): p. 39-55.