doi:10.1017/S1431927620013732

© Microscopy Society of America 2020

# He-ion Beam Imaging for Accurate Hardware Trojan Detection

Nitin Varshney[1], Haoting Shen[2], Olivia Paradis[1] and Navid Asadizanjani[1]

[1]University of Florida, Gainesville, Florida, United States, [2]University of Nevada, Reno, Nevada, United States

Outsourcing integrated circuit (IC) design, fabrication, and test facilities has become common because it reduces costs and time-to-market. Such outsourcing allows external entities full access to all the design details, e.g. GDSII layout and test vectors (test inputs and test responses). As a result, the foundry is left vulnerable to hardware Trojan (HT) insertion from the design house. HT is any malicious modification to the circuit which occurs at any phase of design, integration, or fabrication [1]. Since ICs are prevalent in modern electronic devices, HTs can compromise the security and trustworthiness of critical infrastructures, such as those within the civilian, military, and medical domains [2], [3].

HTs possess a stealthy nature by design, which makes them challenging to detect. There are several different HT detection techniques available in the market and studied by researchers, such as electrical-testing and imaging-based methods. However, as modern ICs become more complex and HTs become more sophisticated, such HT detection techniques quickly become out-of-date because they lack the coverage, speed, and/or confidence of detection. For example, consider the state-of-the-art Trojan Scanner (TS), an imaging-based partial reverse engineering approach to detect HTs that is supported by modern microscopies and AI-enhanced image analysis [2]. The full, traditional TS process flow is detailed in Fig. 1 [2]. Unfortunately, TS suffers from a stark trade-off between detection accuracy and time. Faster scanning electron microscope (SEM) imaging produces noisier images, which are difficult to process with advanced computer vision methods and causes a significant performance drop. To mitigate this accuracy/time tradeoff, we introduce leveraging He-ion imaging instead of SEM. A proof-of-concept methodology is detailed in the following paragraphs.

First, a sample IC (Xilinx FPGA-28nm) is prepared as in the traditional TS workflow. Here, the IC undergoes etching, polishing, and ion milling until the heavily doped silicon layer (p+ and n+) is exposed. A simplified schematic of an IC surface under observation is illustrated in Fig. 2a. Here, the silicon with different dopants, doping concentrations, and micro filler cells is shown. Micro filler cells, usually hard metal e.g. W, are inserted to maintain planarity during ultra-precision chemical-mechanical-polishing during IC fabrication. The materials and structures within the active regions require low prime e-beam energy (e.g. 5kV) to prevent surface charging when taking high-quality images. As the sample surface is polished and ion-milled, the image contrast between different regions are attributed to passive voltage contrasts (PVCs), i.e. the varied interactions between secondary electrons and different local materials and surface potentials. In this paper, SEM images were obtained for reference using TESCAN FERA3 secondary electrons (Fig. 2b-left). Here, the filler cells and the heavily doped silicon regions are both visible and are difficult to differentiate. This presents challenges in HT detection, as an adversary can replace the non-functional filler cells with functional doped silicon or vice versa, without being detected.

He-ion focused ion beam (FIB) images were obtained using Zeiss Orion-Nanofab with 25 kV (Fig. 2b-right). Though He-ion images also use secondary electrons, the PVC is different than in SEM. Here, the doped silicon regions are still bright as in SEM, but the filler cells are invisible, as they are indistinguishable from the lightly doped silicon substrate. This is likely because both the filler cells and the lightly doped silicon are not grounded. The positive charges from the ion beam accumulate on the surface of ungrounded regions, build up positive surface potential, and trap the electrons. Therefore,

https://doi.org/10.1017/S1431927620013732 Published online by Cambridge University Press

secondary electron (SE) emission is limited on these regions, which makes these regions appear dark. Meanwhile, as the accelerating voltage is higher in He-ion imaging (e.g. 25 kV), the metal connections beneath the surface allow SE emission, which makes these regions appear bright. Such subsurface features are not visible in SEM images because the SE emission is lower.

HTs can involve malicious insertions at non-connected filler cells as well as replacing the heavily doped silicon with filler cells, therefore maliciously deactivating part of the designed circuit. Both cases are difficult to detect with SEM, as filler cells and heavily doped regions are indistinguishable. However, assuming a golden layout (reference layout) is available, He-ion images are sufficient for detection of both malicious deletions and insertions.

In this paper, approximately 30% of the cells found using SEM on the sample IC were filler cells. Hence, He-ion images reduce the complexity and time to analyze the cells and leads to better accuracy when detecting HTs relative to SEM. Authors will present a detailed image analysis comparing SEM and He-ion images in future work.

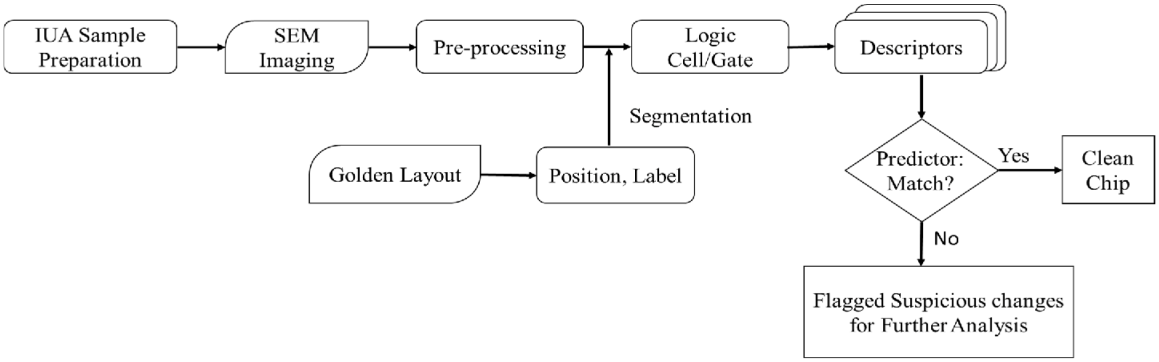

**Figure 1.** State-of-the-art Trojan Scanner Workflow [2]

https://doi.org/10.1017/S1431927620013732 Published online by Cambridge University Press

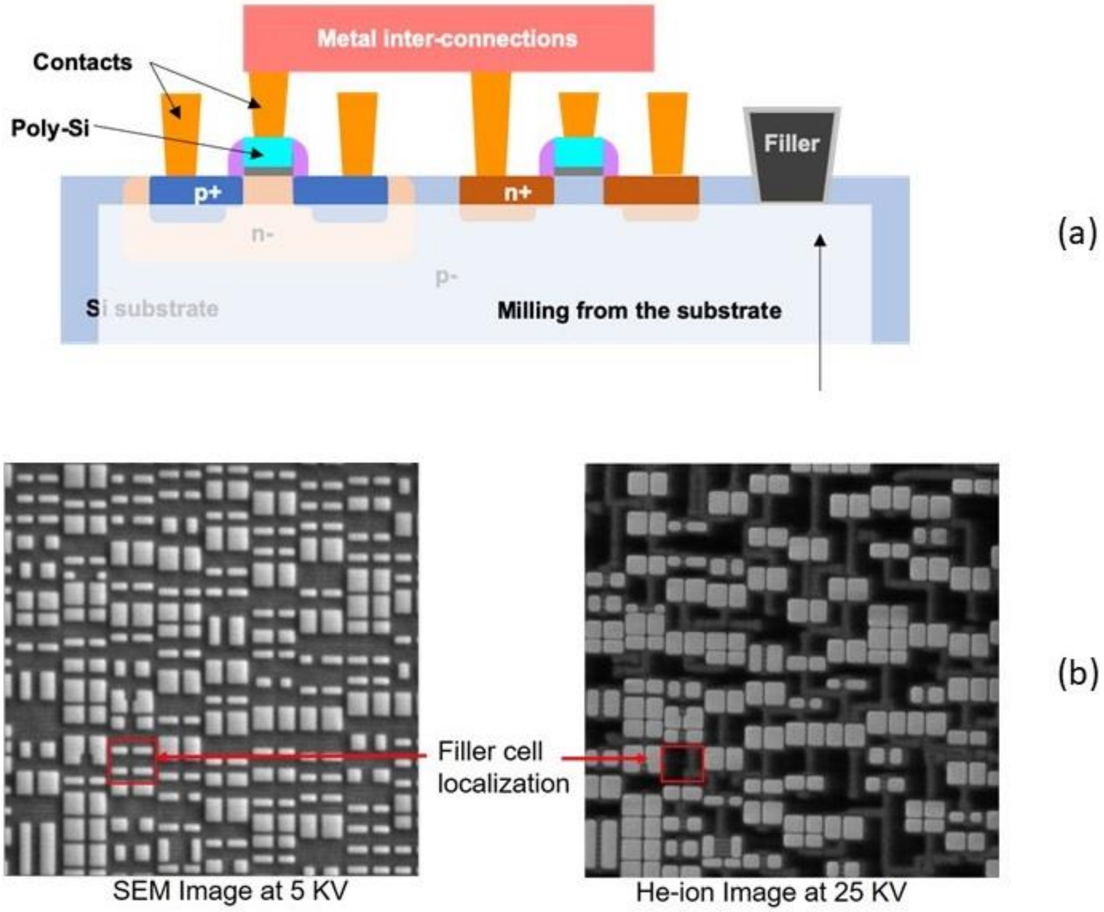

**Figure 2.** 2.(a). Schematic of IC cross-section (b) SEM and He-ion images of IC. An example of filler cells that are visible in the SEM image but not in the He-ion image is marked with red rectangles. Locations of filler cells are non-essential for HT Detection

References

[1]. M. Tehranipoor and F. Koushanfar, “A survey of hardware trojan taxonomy and detection,” IEEE design & test of computers, vol. 27, no. 1, pp. 10–25,2010.

[2] N. Vashistha, H. Lu, Q. Shi, M. T. Rahman, H. Shen, D. L. Woodard, N. Asadizanjani, and M. Tehranipoor, “Trojan scanner: Detecting hardware trojans with rapid SEM imaging combined with image processing and machine learning,” in ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis. ASM International, 2018, p. 256.

[3] M. T. Rahman, Q. Shi, S. Tajik, H. Shen, D. L. Woodard, M. Tehranipoor, and N. Asadizanjani, “Physical inspection & attacks: New frontier in hardwar esecurity,” in2018 IEEE 3rd International Verification and Security Workshop (IVSW). IEEE, 2018, pp. 93–102