REFICS: A Step Towards Linking Vision with Hardware Assurance
-Supplementary Material-

Ronald Wilson, Hangwei Lu, Mengdi Zhu, Domenic Forte and Damon L. Woodard
Florida Institute for Cybersecurity Research (FICS), University of Florida
Gainesville, FL 32601, USA
ronaldwilson@ufl.edu

1. Robustness of the Synthetic Image Generation Workflow

RE-assisted hardware assurance is a complicated process. It involves physical interaction with the sample material which may induce more errors in addition to the imaging modality based sources of noise. For instance, the sample maybe contaminated by dust particles which may hide critical features in the IC during imaging. However, the simplified simulation workflow, shown in Figure 1, only includes the imaging modality based sources of noise. Modelling the entire RE process using such a simplified simulation model may raise questions concerning the robustness and generalizability of the workflow. To this end, a comprehensive list of sources of error inducing noise in the RE process was compiled from existing literature and case studies.

Source of Error	Relevant work
Beam Interaction	[10, 15, 5, 20, 24, 1, 25]
Radiation Damage	[22]
Beam Drift	[4, 3]
Residue	[2]
Uneven delayering	[8, 22]
Die warpage	[17, 26]
Conduction	[8, 16, 18, 11]
External contaminants	[4, 9]
Stitching	[13, 19, 28]
Vertical alignment	[12]
Flicker Noise	[27]
Oxidation	[23]
Electromigration	[6, 14]
Process variations	[21]
Incorrect information	[7]

Table 1. Works describing the sources of errors in RE

The list is organized in Figure 2. The taxonomy of noise sources is essential in understanding the RE process but their influence and impact on the RE workflow can only be classified by their nature of interaction with the process; either predictable or random. The "*imaging-related*" sources of error in the taxonomy incorporates the noise sources from the imaging modality and the errors that result as a direct consequence of physical interaction with the IC sample. The noise introduced in the RE workflow as a consequence of the design practices and materials used in manufacturing the IC is listed as "*Foundry/Node technology-specific*" sources of error. Finally, the errors that occur due to human interactions is listed under "*human factors*". The source literature discussing these noise sources also introduce approaches to suppress it. For instance, conduction in imaging-related sources of error can be prevented by depositing thin layers of conductive materials such as carbon or platinum on the IC die surface [18, 11]. A detailed discussion on the individual noise sources, except for layout-specific sources of errors, are foregone to avoid redundancy. Layout-specific error sources, such as feature dimensions and proximity, are a direct result of the layout synthesis and so-called design rules. Complex geometry of structures can only be imaged if they are within the resolution capability of the imaging modality. Similarly, structures placed in close proximity with each other may, also, not be resolved effectively. In simpler terms, these features may be truncated by the SEM unless a small Field-of-View or high magnification is used. Works discussing each source of error and the approach for resolving it is shown in Table 1. Comprehensive model validation is also provided in the cited works. The sources of errors that cannot be suppressed or prevented are included as part of the synthetic image generation workflow to populate the dataset.

Another concern can be raised on the limited selection of design layout used for generating the dataset. The basic building blocks of any digital design are the standard cells. These represent basic logic gates, more complex gates (e.g., full adders), and registers, and are repeated throughout the design. Popular commercial IC design tools and an open-source standard cell library (both licensed from Synopsys for generating the dataset) are used to synthesize and place-and-route the Advanced Encryption Standards (AES) design. The tools are guided by the design rules specified in the 90nm and 32/28nm process design kits (PDKs) respec-

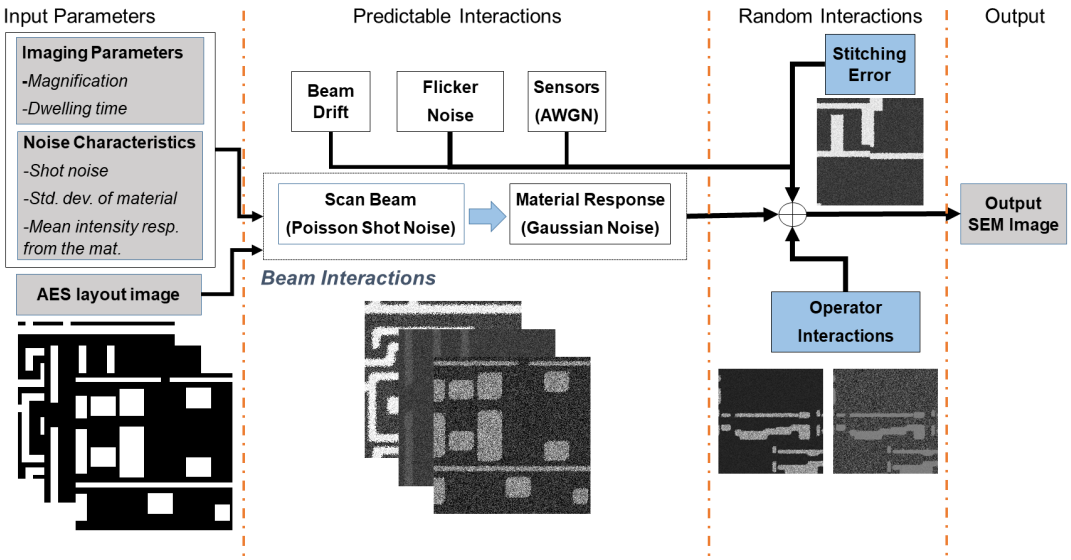

Figure 1. Workflow for generating a synthetic SEM image for the REFICS dataset.

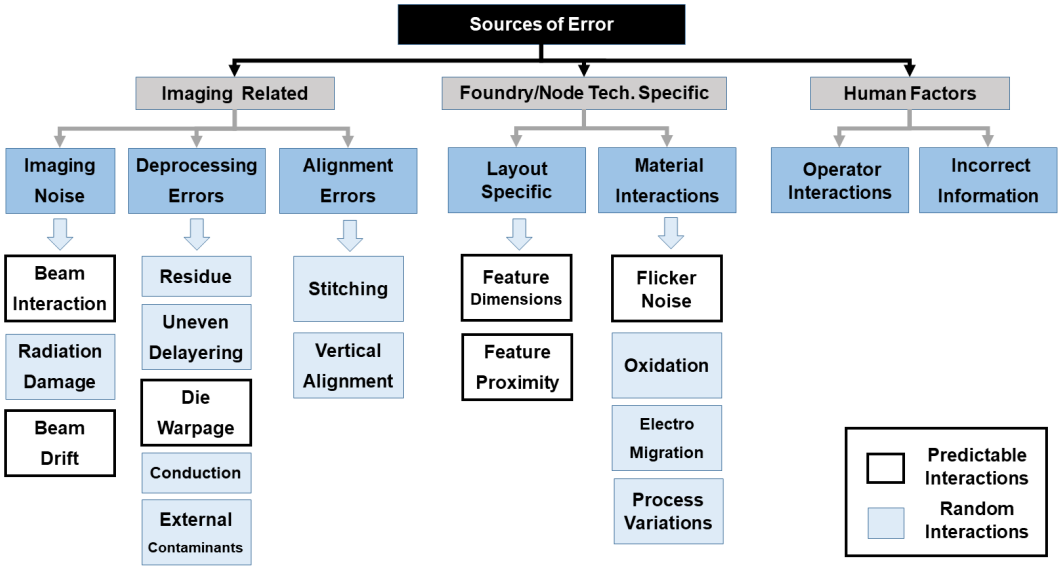

Figure 2. Taxonomy of various noise sources affecting image quality and reliability in the RE workflow

tively. Since the same design rules and standard cells would be used by the tools for any design, including a contemporary processor, the influence of the limited design layouts on the viability of the dataset will be minimal. To further address this concern, a tool is provided along with the dataset to generate SEM images from a new design layout.

2. Experimental Setup for Model Validation

A smart card IC was deprocessed to satisfy the real SEM image data requirement for the experiment. A 250μm window was opened on the flip-side of the IC using a Focused Ion Beam and images were acquired using a 25μm Field-of-View and dwelling times of 10 and 3.2μsec/pixel. With a fixed resolution of 1024$\times$1024 pixels, 25 SEM images of the diffusion layer were captured for each dwelling time setting. These images were hand-labelled as pixels belonging to either the silicon substrate or the doped region. For the Monte Carlo simulation counterpart in the experiment, the imaging parameters used were the the shot noise (λ_{shot}) value for the primary scanning beam, and, the expected mean (μ_{mat}) and standard deviation (σ_{mat}) for the pixel intensity response from the material under study. For obtaining a single pixel value, using the beam interaction model i.e. the scanning beam (PE) and the corresponding response (SE), from the material in the SEM is shown in Equations

1 and 2. The simulation generated 64,000 pixels for every possible combination of the parameters listed in the paper. The comparison between the real and synthetic SEM image can now be performed.

$$PE = Poisson(\lambda_{shot}) \tag{1}$$

$$SE = Gaussian(\mu_{mat} \pm k \times 2.5 \times \sigma_{mat}, \sigma_{mat}) \tag{2}$$

$$\text{where, } k = \frac{PE}{max(PE) - min(PE)}$$

In image processing and computer vision, the similarity between images are assessed using two distinct characteristics of the image: the image histogram and texture. In both cases, the data preparation follows the same process. Initially, a hand-labelled ground-truth image is taken and the labelled pixels are filled in by sampling the pixel values generated by the Monte Carlo simulation to produce a synthetic image representing the particular set of image simulation parameters. This is repeated for every possible combination of simulation parameters. The mean pixel intensity values for the silicon substrate and the doped region were used to offset the histogram for the simulated images. For instance, silicon substrate and the doped region had a mean pixel intensity value of 60 and 161 respectively in our real SEM image data. For assessing the similarity in image histogram, the image histogram (pixel intensity frequency distribution) of the real SEM image and the corresponding synthetic SEM images representing every combination of simulation parameters are taken. The similarity between image histograms were assessed using the Jensen-Shannon distance. A distance value of zero indicates that both the histograms are the same. Similarly, for assessing the similarity in image texture, the real SEM images and the synthetic SEM images were decomposed using the Fourier transform. The magnitude spectrum for both images were rearranged into vectors and the similarity was assessed using the cosine distance between the two vectors. Both the experiments produced identical results. Similarity in histogram of the images suggest that the distribution from which the pixels are sampled are identical. Further, with the Fourier domain representation of the images being identical, the relationship of a pixel with its neighbouring pixels (i.e. the texture) is preserved as well. These observations, along with the model validations reported in literature, suggests that the real and synthetic SEM images are very similar.

The real SEM images of the IC, used for validating the model, will not be a part of the dataset due to intellectual property limitations. However, in a planned future expansion of the dataset, SEM images extracted from a real contemporary IC designed in-house will be provided.

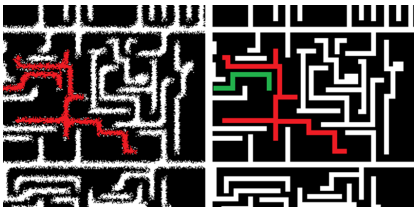

Figure 3. Imperfections introduced by the segmentation algorithms. Tiny hairline connection exists between the red components highlighted on the left leading to a false short circuit (under-segmentation). Original layout is shown on the right for comparison.

3. Metrics

There are several metrics used in RE-assisted hardware assurance. SSIM, IoU and MSE are the most common. SSIM captures the shape information about the structures in the image. MSE looks at pixel-level accuracy. However, they do not contain any contextual information. For instance, in a 250×250 segmented image, a hairline segmentation error, shown in Figure 3, may only span five pixels and MSE would deem this as a near perfect segmentation of the SEM image. However, this error would change the functionality of the entire IC. Similarly, IoU looks at the placement of each structure in the image. These metrics do not capture the intricacies of RE. Consequently, two additional custom metrics were added to the evaluation criteria.

Connected component (CC) analysis is a common technique in image analysis. This measure looks at the connectivity between every pixel to its neighbours. If a segmentation error exists, unintentionally connecting or disconnecting structures in the image (a hairline segmentation error connecting two metal traces for instance), it can be captured using the CC measure. For CC, a 4-connected component analysis is performed. In 4-connected components analysis, two pixels in the image are said to be connected if an odd-sized kernel placed on one of the pixels is horizontally or vertically adjacent to the other pixel, i.e., is in its neighbourhood. The connectivity is analyzed for ever pixel in the image and used to determine if any two structures in the segmented image is connected. The same process is repeated for the ground-truth image as well. The ratio of false open-circuit structures to the total number of structures in the image represents over-segmentation/false open-circuit (CC-OS). Similarly, the ratio of false short-circuit structures to the total number of structures in the image represents under-segmentation/false short-circuit (CC-US). In a perfectly segmented image, both of these scores will be zero.

4. Dataset Examples

Figure 4 presents a few samples from the REFICS dataset. The dataset contains images for two node tech-

nologies and four layers. The segmented ground truth, the layout mask that including the stitching error, and raw SEM images are provided.

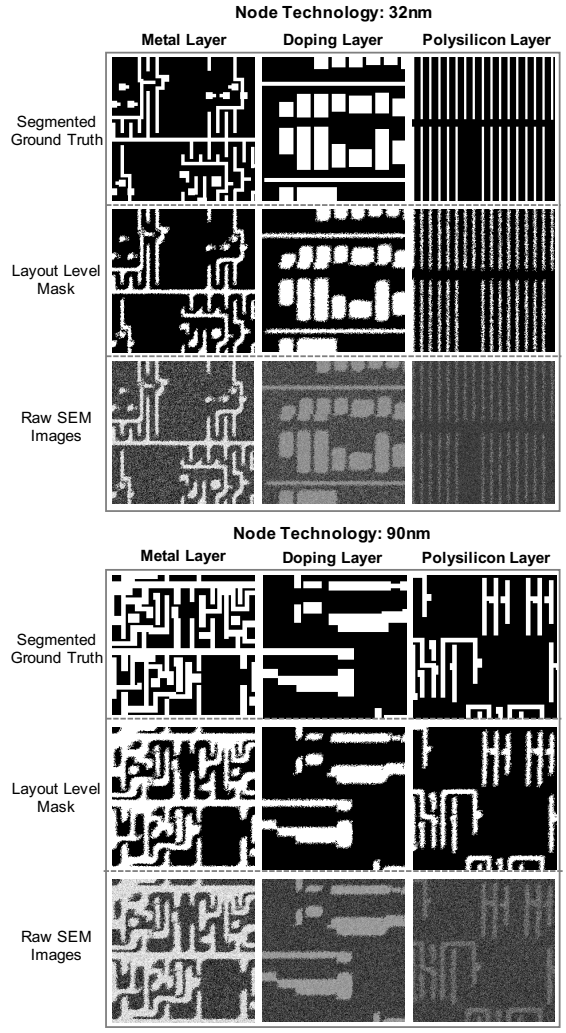

Figure 4. Samples from REFICS dataset.

5. Output Examples from End-to-end Networks

Figure 5 presents the example output from four end-to-end deep neural networks. CBDNet restores small features and sharp edges better than DnCNN. Pix2pix and cycleGAN tend to translate the image style to have sharp edges, but they miss pixels on small features.

Figure 6 presents a few imperfect cases generated from networks. The low contrast case shown in Figure 6(a) is the most challenging, where the patterns in the raw SEM image is barely perceptible. This is most likely to happen in the polysilicon layer. Figure 6(b) presents the performance of networks on restoring stitching errors. The observed inconsistency may affect particular applications. For example, it may not affect Trojan detection methods that rely on representative features but it will affect that rely on template matching.

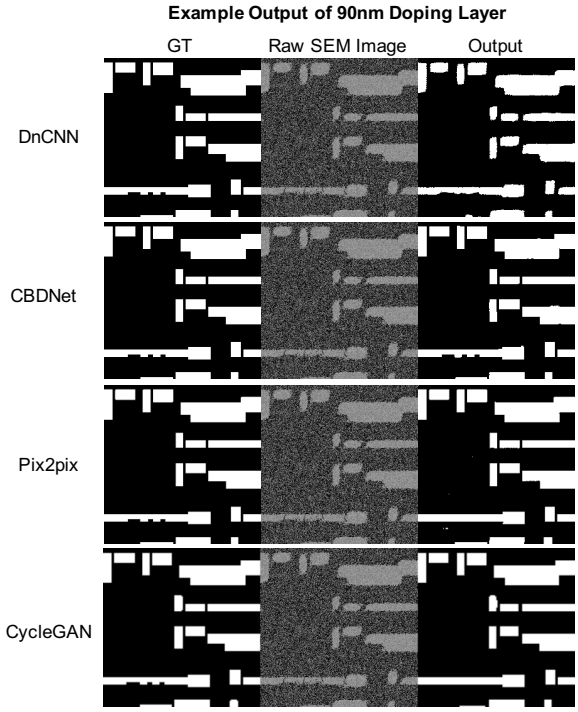

Figure 5. Example output for the same testing image.

On a side note, the algorithms, including deep learning models, used for bench-marking the dataset use the parameters used in the source works. The intention of the benchmarks is to provide a baseline for building better vision algorithms and insights into the problem rather than optimizing the performance for each algorithm.

References

[1] Christopher F Batten. Autofocusing and astigmatism correction in the scanning electron microscope. *Mphill thesis, University of Cambridge*, 2000.

[2] Ulbert J Botero, Ronald Wilson, Hangwei Lu, Mir Tanjidur Rahman, Mukhil A Mallaiyan, Fatemeh Ganji, Navid Asadizanjani, Mark M Tehranipoor, Damon L Woodard, and Domenic Forte. Hardware trust and assurance through reverse engineering: A survey and outlook from image analysis and machine learning perspectives. *arXiv preprint arXiv:2002.04210*, 2020.

[3] Narendra Chaudhary, Serap A Savari, and Sai S Yeddulapalli. Line roughness estimation and poisson denoising in scanning electron microscope images using deep learning. *Journal of Micro/Nanolithography, MEMS, and MOEMS*, 18(2):024001, 2019.

[4] Petr Cizmar, András E Vladár, Bin Ming, Michael T Postek, National Institute of Standards, and Technology. Simu-

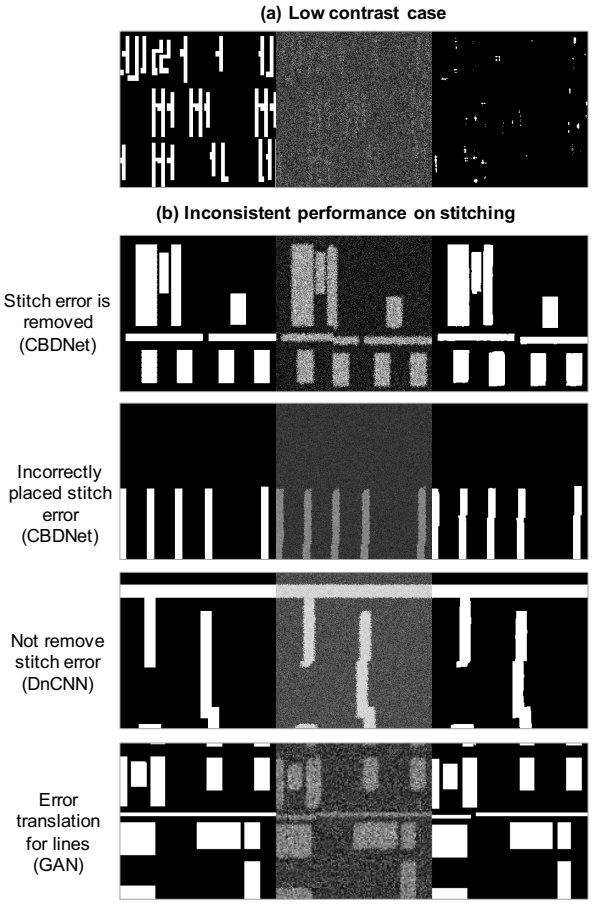

Figure 6. Inaccurate reconstruction cases.

lated sem images for resolution measurement. *Scanning*, 30(5):381–391, 2008.

[5] Luděk Frank. Noise in secondary electron emission: the low yield case. *Journal of electron microscopy*, 54(4):361–365, 2005.

[6] Sean P Frigo, Zachary H Levine, and Nestor J Zaluzec. Submicron imaging of buried integrated circuit structures using scanning confocal electron microscopy. *Applied Physics Letters*, 81(11):2112–2114, 2002.

[7] Marc Fyrbiak, Sebastian Strauß, Christian Kison, Sebastian Wallat, Malte Elson, Nikol Rummel, and Christof Paar. Hardware reverse engineering: Overview and open challenges. In *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*, pages 88–94. IEEE, 2017.

[8] LR Harriott, A Wagner, and F Fritz. Integrated circuit repair using focused ion beam milling. *Journal of Vacuum Science & Technology B: Microelectronics Processing and Phenomena*, 4(1):181–184, 1986.

[9] Xuenong Hong, Deruo Cheng, Yiqiong Shi, Tong Lin, and Bah Hwee Gwee. Deep learning for automatic ic image analysis. In *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*, pages 1–5. IEEE, 2018.

[10] Stephen Kockentiedt, Klaus Tönnies, Erhardt Gierke, Nico Dziurowitz, Carmen Thim, and Sabine Plitzko. Poisson shot noise parameter estimation from a single scanning electron microscopy image. In *Image Processing: Algorithms and Systems XI*, volume 8655, page 86550N. International Society for Optics and Photonics, 2013.

[11] Jin Won Koh, Gu Teak Hwang, Moon Seop Hyun, Jun-Mo Yang, and Jeoung Woo Kim. Semiconductor layer extraction techniques by sem. In *18th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–3. IEEE, 2011.

[12] Tong Lin, Yiqiong Shi, Na Shu, Deruo Cheng, Xuenong Hong, Jingsi Song, and Bah Hwee Gwee. Deep learning-based image analysis framework for hardware assurance of digital integrated circuits. In *2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–6. IEEE, 2020.

[13] Bernhard Lippmann, Michael Werner, Niklas Unverricht, Aayush Singla, Peter Egger, Anja Dübotzky, Horst Gieser, Martin Rasche, Oliver Kellermann, and Helmut Graeb. Integrated flow for reverse engineering of nanoscale technologies. In *Proceedings of the 24th Asia and South Pacific Design Automation Conference*, pages 82–89. ACM, 2019.

[14] DW Malone and RE Hummel. Electromigration in integrated circuits. *Critical Reviews in Solid State and Material Sciences*, 22(3):199–238, 1997.

[15] James Pawley and Heide Schatten. *Biological low-voltage scanning electron microscopy*. Springer, 2007.

[16] Michael T Postek and AE Vladar. Is low accelerating voltage always the best for semiconductor inspection and metrology? *Microscopy and Microanalysis*, 9(S02):978–979, 2003.

[17] EL Principe, Navid Asadizanjani, Domenic Forte, Mark Tehranipoor, Robert Chivas, Michael DiBattista, Scott Silverman, Mike Marsh, Nicolas Piche, and John Mastovich. Steps toward automated deprocessing of integrated circuits. In *ISTFA 2017: the 43rd International Symposium for Testing and Failure Analysis*, page 285. ASM International, 2017.

[18] Raul Quijada, Roger Dura, Jofre Pallares, Xavier Formatje, Salvador Hidalgo, and Francisco Serra-Graells. Large-area automated layout extraction methodology for full-ic reverse engineering. *Journal of Hardware and Systems Security*, 2(4):322–332, 2018.

[19] R. Quijada, A. Raventós, F. Tarrés, R. Durà, and S. Hidalgo. The use of digital image processing for ic reverse engineering. In *2014 IEEE 11th International Multi-Conference on Systems, Signals Devices (SSD14)*, pages 1–4, 2014.

[20] Makoto Sakakibara, Makoto Suzuki, Kenji Tanimoto, Yasunari Sohda, Daisuke Bizen, and Koji Nakamae. Impact of secondary electron emission noise in sem. *Microscopy*, 68(4):279–288, 2019.

[21] Esha Sarkar and Michail Maniatakos. On automating delayered ic analysis for hardware ip protection. In *Proceedings of the International Conference on Omni-Layer Intelligent Systems*, pages 205–210. ACM, 2019.

[22] H Seiler. Secondary electron emission in the scanning electron microscope. *Journal of Applied Physics*, 54(11):R1–R18, 1983.

[23] Marek Sikul, Karel Novotny, Matthias Kemmler, and Andreas Rummel. Sem-based nanoprobing on in-situ delayered

advanced 10 nm technology node ic. In *2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–4. IEEE, 2018.

[24] KS Sim, JTL Thong, and JCH Phang. Effect of shot noise and secondary emission noise in scanning electron microscope images. *Scanning: The Journal of Scanning Microscopies*, 26(1):36–40, 2004.

[25] F Timischl, M Date, and S Nemoto. A statistical model of signal–noise in scanning electron microscopy. *Scanning*, 34(3):137–144, 2012.

[26] Sebastian Wallat, Nils Albartus, Steffen Becker, Max Hoffmann, Maik Ender, Marc Fyrbiak, Adrian Drees, Sebastian Maaßen, and Christof Paar. Highway to hal: open-sourcing the first extendable gate-level netlist reverse engineering framework. In *Proceedings of the 16th ACM International Conference on Computing Frontiers*, pages 392–397, 2019.

[27] Ronald Wilson, Hangwei Lu, Mengdi Zhu, Domenic Forte, and Damon L Woodard. Refics: Assimilating data-driven paradigms into reverse engineering and hardware assurance on integrated circuits. *IEEE Access*, 2021.

[28] David Zhang, Gooitzen van der Wal, Phil Miller, David Stoker, Erik Matlin, Naveen Marri, Gary Gan, Joe Zhang, Jane Asmuth, Sek Chai, et al. Fast, full chip image stitching of nanoscale integrated circuits. Technical report, SRI International Princeton United States, 2019.