

ML Assisted Authentication via Tampered Optical Responses

A deep-learning optical-PUF system that distinguishes tampering from degradation with ~97.6% accuracy for anti-counterfeit chip security.

Technological advancements have enabled the semiconductor industry to grow into a market worth over \$500 billion. In parallel, counterfeiting techniques have advanced as well, leading to a market of counterfeit semiconductor chips worth \$75 billion. Therefore, to maintain the security and safety of a world that is dependent on semiconductor technologies, the ability to take active measures in counterfeit detection has emerged as a promising field of advancement. Current methods in detection rely on identifying physical unclonable functions (PUFs), which leverage unique signatures of physical systems like semiconductor chips. Optical PUFs use the interactions between materials and light to create and identify a distinct signature. While effective, current methods using optical PUFs struggle to differentiate between intentional tampering rather than natural degradation or other environmental factors that could affect the material.

In response to this challenge, researchers at Purdue University have developed RAPTOR, a method to unlock extreme accuracy in tampering detection by analyzing gold nanoparticle patterns embedded on chips. The unique patterns act as an optical PUF which can be authenticated using the method. The method applies a novel deep-learning approach that can adapt to a chip's complex environment to properly discern between natural changes in nanoparticle distributions versus distinct tampering. As a result, the method has achieved a detection accuracy of 97.6% under worst-case scenario tampering assumptions. This surpasses current analytical methods and reveals a clear path to integrate machine-learning based tampering detection methods to advance and secure the semiconductor industry in an advancing world.

Technology Validation:

The accuracy and speed of the RAPTOR method was compared to other known methods of optical PUF authentication utilizing random data samples

Technology ID

2024-BOLT-70652

Category

Computing/Photonic & Optical

Computing Technologies

Chemicals & Advanced

Materials/Materials Processing &

Manufacturing Technologies

Further information

Will Buchanan

wdbuchanan@prf.org

View online page



of gold nanoparticles. It achieved 97.6% accuracy within the tested group.

Advantages:

- Generates data sets for gold nanoparticle PUFs for future machine learning applications
- High verification accuracy of 97.6% compared to traditional methods in difficult, worst-case scenario condition assumptions

Applications:

- Semiconductor manufacturing industry technologies
- Machine learning and algorithm development

Publications:

Blake Wilson, Yuheng Chen, Daksh Kumar Singh, Rohan Ojha, Jaxon Pottle, Michael Bezick, Alexandra Boltasseva, Vladimir M. Shalaev, Alexander V. Kildishev, "Authentication through residual attention-based processing of tampered optical responses," Adv. Photon. 6(5) 056002 (17 July 2024)
<https://doi.org/10.1117/1.AP.6.5.056002>

Blake Wilson, Yuheng Chen, Daksh K. Singh, Rohan Ojha, Michael Bezick, Jaxon Pott, Vladimir M. Shalaev, Alexandra Boltasseva, Alexander V. Kildishev, "Machine-learning-assisted optical authentication of chip tampering," Proc. SPIE PC13113, Photonic Computing: From Materials and Devices to Systems and Applications, PC131130E (3 October 2024);
<https://doi.org/10.1117/12.3027858>

<https://www.purdue.edu/newsroom/2024/Q3/purdue-deep-learning-innovation-secures-semiconductors-against-counterfeit-chips/>

<https://stories.prf.org/raptor-takes-a-bite-out-of-global-counterfeit-semiconductor-market/>

TRL: 4

Intellectual Property:

Provisional-Patent, 2024-06-11, United States

Utility Patent, 2025-06-10, United States

Explore other available products test at [The Office of Technology Commercialization Online Licensing Store](#)

Keywords: Electrical Engineering, LEDs, Materials and Manufacturing,
Perovskite, semiconductor manufacturing, Semiconductors