IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 19, 2020, accepted March 26, 2020, date of publication April 10, 2020, date of current version April 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987088

Gate-Level Validation of Integrated Circuits With Structured-Illumination Read-Out of Embedded Optical Signatures

NEGIN ZARAEE[1], (Student Member, IEEE), BOYOU ZHOU[1], KYLE VIGIL[2], MOHAMMAD M. SHAHJAMALI[3], AJAY JOSHI[1], (Senior Member, IEEE), AND M. SELIM ÜNLÜ[1,2,4], (Fellow, IEEE)

[1]Department of Electrical and Computer Engineering, Boston University, Boston, MA 02215, USA
[2]Department of Physics, Boston University, Boston, MA 02215, USA
[3]School of Engineering and Applied Sciences, Harvard University, Cambridge, MA 02138, USA
[4]Department of Biomedical Engineering, Boston University, Boston, MA 02215, USA

Corresponding author: M. Selim Ünlü (selim@bu.edu)

This work was supported in part by the National Science Foundation under Grant EECS-1641018, and in part by Boston University Ignition Award and Honeywell.

ABSTRACT The integrated circuit (IC) chips are essential components in a variety of computing systems ranging from consumer electronics to high-security military devices. Hence, the authenticity of ICs is crucial. The pervasive nature of ICs and the need for their low-cost production has led to the globalization of IC design and manufacturing process, which has raised various security concerns including; (i) malicious tampering of ICs during fabrication to include Hardware Trojans (HT); and (ii) IC counterfeiting. To detect HTs and IC counterfeiting, we require an examination method to ensure the manufactured IC is consistent with the intended design. Here, we present a robust, rapid, and nondestructive IC authentication technique, which relies on imaging the optical watermarks embedded in predetermined locations in the IC. The watermark is a combination of unique signatures in the optical farfield reflection pattern created by modifying the physical layout of logic gates. These high-contrast optical signatures are enabled by embedding an innovative combination of plasmonic nanoantennas and grating structures directly in the metal-1 layer of the gate design. The uniqueness of logic gates' optical signatures is ensured through different plasmonic nanoantenna dimensions and periodicity of the surrounding gratings. For the rapid read-out of the watermarks, we present a confocal dark-field imaging technique utilizing modulated structured-illumination and lock-in signal acquisition. By combining these innovations in plasmonic nanoantennas and optical imaging, we demonstrate through numerical simulations a 30-fold contrast in polarization dependent reflectivity for each embedded optical signature allowing rapid read-out of watermarks and direct authentication of the IC design.

INDEX TERMS Back-side imaging, hardware trojan detection, IC counterfeit detection, integrated circuits, interference, lock-in measurement, plasmonic nanoantenna, structured-illumination.

I. INTRODUCTION

A. BACKGROUND AND MOTIVATION

Integrated Circuit (IC) chips are increasingly ubiquitous in today's networked and information-driven systems. Semiconductor technology has enabled the development of IC chips for computation, storage, sensing and communications with broad utilization in diverse areas from personal connectivity to healthcare, and from entertainment to municipal facilities [1, 2]. We can no longer imagine a world without smart and networked devices as illustrated by the emergence of the Internet of Things (IoT). For the IoT to thrive, we require IC chips to function correctly and securely [3] as they are the Root of Trust (RoT). Consequently, the reliability and trustworthiness of IC chips are of utmost importance, especially due to the recent smartphone security issues at the international level. In our work, we specifically focus on identifying counterfeit IC chips and detecting Hardware

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

Trojans (HTs). Here we first identify the limitations of current techniques for IC security evaluation and then propose a new technique built on backside imaging of embedded optical nanoantennas using structured-illumination microscopy.

With the ever-increasing IC chip complexity, the validation of the authenticity of the IC chip has become very challenging. As the fabrication capabilities of semiconductor devices have evolved, the physical dimensions of transistors and logic gates (the building blocks of ICs) have shrunk from several micrometers half a century ago to tens of nanometers today. With nanoscale feature dimensions, we can fit close to 30 million transistors on a fingernail-sized device [4] resulting in more than a billion transistors on a single chip [5]. The security concern due to the nanometer size of circuit elements is exacerbated by the sheer number of transistors on an IC chip. Validating these nanoscale structures is not an easy task.

Traditionally, all the logic designs are verified through electrical testing using digital automated vectors generated by a testing platform [6]. The platforms usually consist of a Field-Programmable Gate Array (FPGA) and the device under test (DUT). The FPGA generates the test vectors that are fed to the DUT. The output of the DUT is then compared with the pre-calculated results. These verification tests need to be designed such that they can capture all bugs, meaning that the test vectors can trigger all the possible errors in DUT. By tracing back the test results, the designers can identify the source of error, and correct the erroneous logic based on the test results. This approach is based on the presumption that all possible logic errors will be triggered by testing vectors. However, there are two obstacles in this approach [7], [8]. First, the test vectors cannot always provide complete coverage and so cannot always trigger all the erroneous logic [9]. For example, in a chip with 1,000 input pins (each pin can receive logic 1 or logic 0 as inputs), the number of possible input combinations is 2^{1000}, which is more than the number of atoms in the universe. Second, logic states are time-dependent, meaning that some logic events cannot be triggered before a period of time has passed [8]. For example, if the triggering of an event is dependent on a capacitance-based timer (for example the event is triggered after the capacitor is fully charged/discharged) the event may not be triggered during the testing time. These obstacles severely limit the scalability of current verification techniques.

To overcome the limitations of traditional electrical testing, a variety of direct circuit imaging/visualization technologies, ranging from electron microscopy to thermal and acoustic imaging, have been implemented [5], [6], [10]–[12]. Transmission Electron Microscopy (TEM) with its exquisite spatial resolution allowing for direct visualization of the nanoscale circuits in detail provides an intuitive method and can be considered as the gold standard [13], [14]. Yet, the complexity, cost and low throughput of TEM hinders its applicability for authentication. Thermal imaging utilizes predefined test vectors to activate thermal traces on the chip for authentication [7], but it has similar limitations to electrical testing. Inadequate spatial resolution in acoustic and electromagnetic imaging limits their applicability for authentication of modern ICs [5], [10], [11].

B. RELATED WORK

Several recent studies have proposed techniques based on utilizing the near-Infrared light to image the logic gates from the backside of an IC [15], [16], [17]. Zhou *et al.* proposed a fast, accurate optical imaging technique that leverages the opaqueness of the metal fill cells to identify any modification of the IC chip layout [16]. The signatures of the embedded structures are identical since the embedded structures are only metal fillings in the fill cells. Therefore, the signatures generated from these cells are not distinguishable from each other.

Adato *et al.* proposed a dictionary-based optical imaging technique [17], where they showed that by inserting a nanoantenna randomly in the gate design and using multi-spectral low-resolution measurements, the classification accuracies of a logic gate can be improved. However, this dictionary-based technique is only applied on a limited number (specifically 6) of gates. To apply this dictionary-based gate classification method to other standard gates in that library as well as to other libraries, we will need to improve the imaging technique effectively. A more accurate technique needs to be developed for reliably imaging logic gates and robustly classifying them.

In this study, we extend the dictionary-based verification method [17] and achieve a 30× improvement on the gate farfield reflection response. This strong enhancement is due to the engineered placement of the nanoantenna into the empty spaces between two gates, instead of adding nanoantenna randomly inside original gate design [17].

C. PROPOSED METHOD

In this study, we propose a backside optical imaging technique based on structured-illumination microscopy to perform IC chip authentication. The IC authentication is achieved by reading out its optical watermark, which is built from a combination of the IC's logic gates' optical signatures. The effectiveness of our proposed IC authentication technique is shown through numerical simulation in this study. In order to understand the basis of this method we first need to have a clear understanding of the IC chips' structure.

As shown schematically in Fig. 1a, IC chips consist of multiple layers assembled on top of a silicon substrate. The metal 1 layer is used to connect the transistors within a logic gate, and the upper layers are used for interconnections between the logic gates [18].

In the back-side imaging setup, we measure the light reflected primarily by metal 1 layer. For the illumination light to penetrate into the Silicon substrate from the back side of the IC, the wavelength should be in the near-infrared regime where Silicon is transparent. Our method leverages the differences in the metal structure of each gate, which can be further optimized by inserting nanoplasmonic features to obtain a unique optical reflection signature as watermarks in ICs.

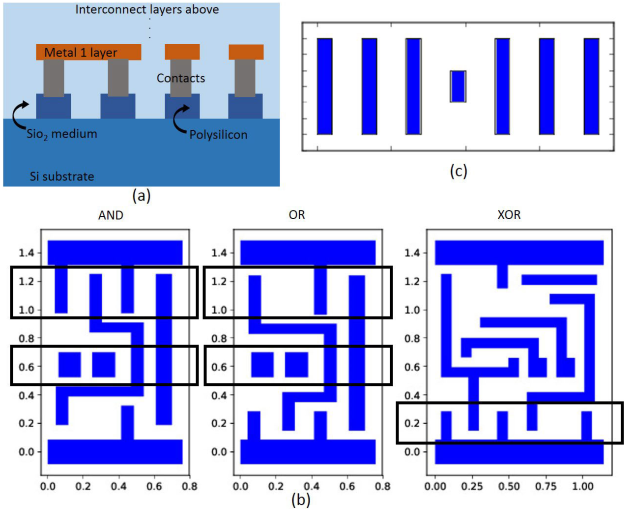

FIGURE 1. Schematics of IC chip layers, example logic gates and designed optical elements. (a) Schematic of Metal 1, contacts and polysilicon layers in an IC. These layers are located on top a Si substrate and embedded in SiO$_2$ medium. (b) From left to right, Metal 1 structures of AND2_X1 gate, OR2_X1 gate, XOR2_X1 gate layout, respectively, with 2 inputs and minimum transistor width. The structures in the Metal 1 layer are shown using blue polygons. Black frames show the potential periodic structures in the gate layout. (c) The designed optical element consisting of the central nanoantenna and surrounding periodic structures on both sides of nanoantenna.

As an example of this general concept, we modify the metal 1 layer layout design of an application-specific integrated circuit (ASIC) by placing an asymmetric plasmonic nanoantenna in between each gate pair (two gates located next to each other) and incorporate the periodic metal bars in their layout to form a grating-like structure which surrounds the nanoantenna. Fig. 1b displays the metal 1 layer layout of AND, OR and XOR logic gates as an example, with the potential periodic structures shown in the black frames. Our proposed optical structures consist of the asymmetric plasmonic nanoantenna that is surrounded by the periodic grating structures as shown in Fig. 1c. The uniqueness of the optical signature of each gate pair is defined by the different dimensions of the nanoantenna and the periodicity of the grating structures surrounding the nanoantenna embedded in various logic gates' layout.

To read-out the embedded optical signatures, we employ a confocal dark-field imaging setup utilizing a structured-illumination consisting of an interference fringe pattern illumination profile. Imaging these different optical signatures depends on choosing the correct illumination parameter set consisting of a specific illumination wavelength and angle. First, by choosing the correct illumination angle we match the periodicity of the illumination fringe pattern with the periodicity of the grating structure embedded in the specific logic gate. Second, we activate the embedded plasmonic nanoantenna in the specific logic gate by matching the illumination wavelength to its dipole plasmon resonance wavelength defined by the nanoantenna dimensions. In addition, due to the asymmetric shape of the plasmonic nanoantenna, the illumination polarization is also a key parameter. We obtain a much stronger farfield response from the nanoantenna when the illumination polarization is along the nanoantenna's long axis.

Therefore, with each illumination parameter set, only specific locations in the IC will light up. These locations correspond to the logic gates that were designed using specific nanoantenna dimension and the grating structure periodicity that would resonate at that specific illumination parameter set. The IC's resulting reflection pattern will create an image resembling a heat map, which will be the IC's watermark. Illuminating the IC with a different illumination parameter set will result in other locations of the IC lighting up. These locations would correspond to logic gates whose designs match the new chosen illumination parameters. Overall, each IC's watermark (i.e. heat map) is unique as it depends on the location of the logic gates in the IC. Two identical ICs built from the same logic gate library (our designed logic gates with modified layout containing the nanoantenna and grating) will give the same reflection map. The goal here is not to differentiate between two identical ICs built from the same logic gate library, but to differentiate between an IC designed using our logic gate library and a modified version (designed by an intruder) of that IC. We achieve IC authentication by comparing the measured far field reflection map of a fabricated IC chip with the IC's expected reflection pattern determined at design time.

Our proposed IC authentication technique is highly distinct from the authentication techniques relying on Physical Unclonable Functions (PUFs). Although, like the first introduced PUF [19], our technique is also an optical method, which relies on the embedded scatterers, the physical principles behind their design and functionality are fundamentally different from ours. Regardless of their type (electronic, optical or magnetic), PUFs are designed to be random and not predictable and they rely on the uncontrollable process variations occurring during the IC manufacturing phase [20, 21]. However, the basis of our approach is predetermined optical responses from our modified logic gate designs. The logic gate modifications performed by embedding our predesigned optical elements in the gate's metal 1 layer layout is done at the design phase and their expected optical response is determined before IC fabrication. In contrast to PUFs, our technique is robust to process variations, ensuring we can achieve the expected optical response from our modified logic gates even in presence of process variations. We discuss the effect of process variations on our methodology in section II (Materials and Methods).

Our technique is potentially applicable to a variety of applications. Here, we present two key applications of our technique: 1) HT detection; and 2) Counterfeit IC chip detection, which is explained in more details in the Discussion section.

II. MATERIALS AND METHODS

In this section, we provide further details on the design parameters that affect the optical signature as well as the illumination and collection optical setup to read-out the designed signatures from the logic gates. In order to specify our optical signatures' required parameters, we first need to know the constraints associated with IC chip imaging. The first constraint is the acceptable functional wavelength regime which is set by both the IC structure/material and the optical setup. For imaging the metal 1 layer of logic gates, we implement back side imaging setup where the gates are illuminated from the Silicon substrate side. For the illumination light to propagate through the substrate and reach the metal layers, we should work in the wavelength regime where Silicon has the lowest absorption, hence allowing most of the light to travel through. Therefore, we work in near-infrared wavelength range, specifically from 1100 nm to 1500 nm, due to the transparency of Silicon in this range [22].

The second constraint is on the material choice of our designed optical structures to obtain the gate's optical signature. Since we are modifying the logic gates' metal 1 layer to incorporate our optical element into the physical layout of the gate, our designed structure should be composed of the same material used to build the metal layers. So, we are bound to work with copper plasmonic nanoantennas.

Finally, the third constraint originates from the IC manufacturing limitations on dimensions of the structures in metal layers. Depending on the technology node, there is a minimum dimension that is physically buildable in the IC. The logic gate designs used in this study are designed using 45 nm technology node, which results in a minimum dimension of 70 nm for the metal structures [23].

A. PLASMONIC NANOANTENNA DESIGN

The first parameter adjustment of the optical signature is the dimensions of the chosen plasmonic nanoantennas. As extensively studied before [24], [25], the localized surface plasmon resonance (LSPR) wavelength of a metallic nanoparticle can be changed by modifying its size. In addition, as shown in previous works [26]–[28], the asymmetric plasmonic nanoantennas generate several orders of magnitude stronger resonance, when illuminated by an electric field polarized along their long axis as compared to that polarized along their short axis. Our asymmetric nanoantennas are designed in a rectangular shape, consistent with IC metal 1 layer structures, with aspect ratios larger than 1.5.

Based on the aforementioned constraints on the material and operational wavelength for back side imaging of IC chips, we identify the copper nanoantenna dimensions that generate their peak dipole plasmon resonance in the near-infrared wavelength range. In order to determine those dimensions, we conduct Finite Difference Time Domain (FDTD) simulations, illuminating a copper rectangular nanoantenna, embedded in SiO_2 medium and placed at a distance of 100 nm from the top surface of a silicon substrate (in order to simulate the surrounding medium's refractive index for the case when this nanoantenna is placed in the layout of the logic gates).

We use the Total-Field-Scattered-Field (TFSF) illumination source and the scattering cross-section analysis group to collect the scattered light from the nanoantenna. Two broadband simulations (from 500 nm to 2500 nm) are performed for each nanoantenna size to acquire the nanoantenna's response for both longitudinal and transverse electric field illumination polarizations. Fig. 2a shows the normalized scattering cross-section spectra of the identified copper nanoantenna sizes, that generate their strong dipole plasmon resonance at our desired wavelength range when illuminated by a longitudinally polarized electric field. The width of all the nanoantennas are fixed at 100 nm and the length changes from 150 nm to 350 nm as shown in Fig. 2a. Note that all the identified nanoantenna dimensions satisfy the constraint of the minimum dimension for our specific technology node (dimensions bigger than 70 nm). It is worth mentioning that the dimension constraint would have not been satisfied for other plasmonic materials such as gold and silver to generate the desired plasmon resonance wavelength range. So the material choice limitation to copper actually works to our benefit.

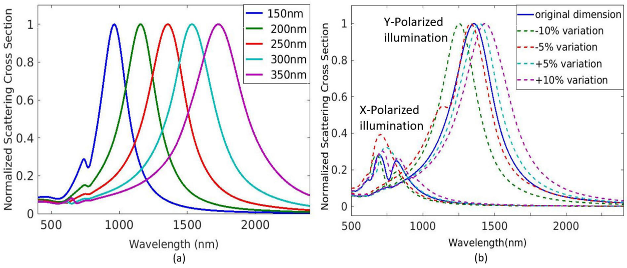

FIGURE 2. Effect of the plasmonic nanoantenna dimension and process variations on its LSPR wavelength. (a) The normalized scattering cross-section of chosen copper nanoantenna dimensions for longitudinal polarized illumination, with a fixed width of 100 nm and varying length as shown in the legends. The nanoantennas are embedded in SiO_2 medium and placed at a distance of 100 nm from the top surface of a silicon substrate (to simulate the surrounding medium refractive index of the case when this nanoantenna is placed in the layout of the logic gates). (b) Blue solid line: The scattering cross-section of nanoantenna dimension (100 nm × 250 nm) when illuminated with longitudinally (Y) and transversely (X) polarized light. Dashed lines: The scattering cross-sections of nanoantenna with dimensions resulting from ±10% and ±5% process variations in the original nanoantenna dimension.

In this manuscript, we have chosen to keep the nanoantenna width at 100 nm as it resonates at our desired wavelength and that size is comparable to the size of the existing metal 1 structures in the logic gates. However, as shown in the Supporting Information, we could achieve these plasmon resonance wavelengths with different nanoantenna dimensions (for example in Fig. S1 the nanoantenna width is fixed at 80 nm and the length is changing).

Fig. 2b shows the strong dependency of the LSPR wavelength of asymmetric nanoantennas on the illumination polarization by comparing the scattering cross-section spectra of a 100 nm × 250 nm copper nanoantenna for the longitudinal and transversal polarized electric field (shown by solid blue curves). As we can see in Fig. 2b, the scattering cross-section spectra corresponding to the transversely polarized illumination generates a much weaker peak at around 700 nm compared to the strong dipole resonance at 1350 nm from the longitudinally polarized illumination. The ratio of the nanoantenna's farfield response to longitudinally polarized electric field illumination (along the long axis of the nanoantenna) to the transverse polarized electric field is the basis of the logic gate's optical signature.

Fig. 2b also shows the effect of process variations on the nanoantenna LSPR wavelength shift. The process variation refers to the naturally occurring variations in width and length of the feature sizes when integrated circuits are fabricated [29]. Fig. 2b shows the scattering cross-section of the nanoantenna dimensions resulting from ±10% and ±5% process variation (typically observed values) in dimensions of the original nanoantenna (100 nm × 250 nm). The LSPR wavelengths of the nanoantennas resulting from −5% and −10% dimension variation (shown by dotted red and green curves, respectively, in Fig. 2b), exhibit a blue shift compared to LSPR wavelength of the original nanoantenna. However, these shifted LSPR wavelengths are still 100 nm and 200 nm, for −10% and −5% variations, respectively, away from the LSPR wavelength of the neighboring chosen nanoantenna dimension (100 nm × 200 nm). The same argument holds for the cases of +5% and +10% dimension variation (shown by dotted light blue and purple curves in Fig. 2b), where the LSPR wavelengths show a red shift from the original LSPR wavelength. However, even after the red shift, there is a difference of around 100 nm and 200 nm between the LSPR of the next chosen nanoantenna dimension (100 nm × 300 nm) and the LSPR of the resulting nanoantenna dimensions from 10% and 5% variations, respectively.

As observed in Fig. 2b, we have intentionally chosen the nanoantenna dimensions for building the optical signatures such that the plasmonic resonance wavelengths are sufficiently far enough from each other, therefore the process variation will not disrupt the signatures. In other words, even in the presence of process variations, various optical signatures built by different embedded nanoantenna dimensions will each generate their unique farfield reflection pattern at only a specific wavelength; thereby, preserving the wavelength dependency of the signatures.

B. DIFFRACTION GRATING DESIGN

The second parameter adjustment required in the proposed optical signature is the periodicity of the grating structures around the nanoantenna. The grating will diffract the incident light at multiple angles depending on the number of allowed diffraction orders. The generated diffraction orders are dependent on the grating period with respect to the illumination wavelength and the illumination angle [30].

Equation (1) describes the diffraction angles of different mode numbers, m, based on the grating period, d, illumination wavelength in the grating's surrounding medium, λ, and the incident angle, θ_i.

$$\theta_m = \sin^{-1}(m\lambda/d - \sin\theta_i). \tag{1}$$

There are multiple factors we should take into account in order to determine the grating structure's period for our optical signatures. First, as observed in Equation (1), for an illumination angle of θ_i with respect to normal direction, the zero-diffraction order ($m = 0$) will diffract at $-\theta_i$, and all the other allowed higher diffraction orders will diffract at smaller angles. Second, in order to read-out the optical signatures, we employ an oblique illumination configuration and perform dark field measurement of the gate's farfield reflection response. This is achieved by collecting only the central 10-degree cone of angles of the reflected light while illuminating the IC chip at 30, 40, 50 and 60 degree incident angles for reading different signatures. Finally, if the higher diffraction orders are allowed in the designed grating structure, they will diffract at smaller angles and end up in the accepted angle range of the collection objective. This diffracted light will overwhelm the collected signal from the nanoantenna and deteriorate the optical signature intensity, which is the ratio of the gate's farfield reflection from longitudinal and transversal illumination polarizations.

Therefore, in order to achieve a stronger optical signature of our modified gate, we choose the grating period such that it will only generate the zero-diffraction order for the chosen illumination wavelength and angle. To achieve only the zero-diffraction order from the grating structures on both sides of the nanoantenna, the constraint on the grating period shown in Equation (2) should be satisfied.

$$d < \lambda/(1 + \sin\theta_i). \tag{2}$$

C. OVERHEAD

The dimensions of the modified logic gate will be larger compared to the original layout of the logic gate, because our proposed IC authentication technique relies on modifying the physical layout of the logic gates to embed the nanoantenna and grating structures. This increase in area causes an increase in the fabrication cost of the IC chip.

To minimize the area overhead we propose to embed our designed optical elements in the layout of a gate pair instead of a single logic gate. We incorporate the asymmetric plasmonic nanoantenna in between two logic gates located next to each other and the grating structures on both sides of the nanoantenna are embedded in the layout of the two neighboring gates. This amortizes that area overhead per logic gate. On an average our nanoantenna and grating structures increase the area of a gate pair by 40%. As part of future work, we plan to develop custom logic gate layouts to reduce this area overhead.

D. ILLUMINATION SETUP DESIGN

We use confocal optical imaging for imaging the IC's watermark. One of the challenges of confocal optical imaging as a scanning technique is the acquisition time that scales with the square of the spatial resolution. We designed the optical system with a confocal spot size on the order of the logic gate dimensions allowing for a fast read-out while maintaining the sensitivity to nanoscale features, embedded in the logic gates, that are much smaller than the illumination spot. Therefore,

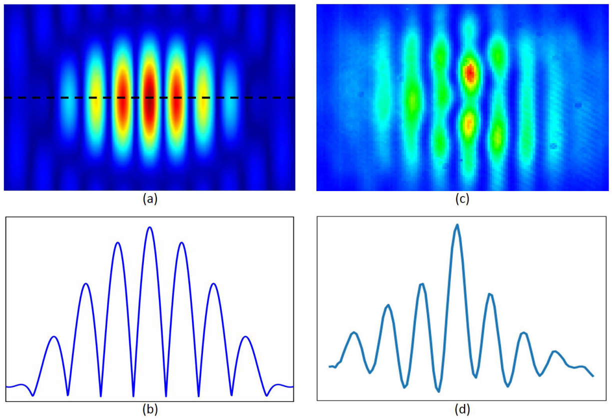

FIGURE 3. Illumination interference fringe pattern. (a) Simulated near electric field Intensity pattern of two Gaussian sources with illumination angles of 40 and −40 degree. The electric field is shown along the plane, 100 nm above the Si/SiO$_2$ interface plane, where the metal 1 layer is located in the simulations. (b) Cross-sectional plot of the illumination profile, along the black dotted line shown in part (a). (c) Illumination fringe pattern generated experimentally using a Spatial Light Modulator (SLM). (d) Cross-sectional plot of the illumination profile generated experimentally in part (c).

we improve the resolution of our imaging system without reducing the illumination spot size; hence, enhancing the image acquisition speed compared to a confocal system with comparable imaging resolution. In this section we present the details of this dark-field confocal structured-illumination imaging setup.

We propose a structured-illumination setup in order to read-out the optical signatures incorporated in the gate's physical layout. The setup consists of two coherent illumination sources at the backside of the IC chip, with θ_i and $-\theta_i$ incident angles, which will interfere and create an interference fringe pattern illuminating the gate's metal 1 layer. We performed Lumerical FDTD simulations to demonstrate our structured-illumination profile. Fig. 3a indicates the fringe pattern resulting from interference of two Gaussian sources with incident angles of 40 and −40 degrees, illuminating the back side of a layered Si/SiO$_2$ substrate. Fig. 3b indicates the cross-sectional plot of the illumination profile along the black line shown in Fig. 3a. The interference pattern consists of periodic peaks and valleys resulting from constructive and destructive interference, respectively, of the two coherent illumination sources.

As shown in Fig. 3c, we have also generated this illumination pattern experimentally using a Spatial Light Modulator (SLM) capable of modulating the phase between two input beams. The pattern is generated by illuminating two spots on opposite sides of the back focal plane of the microscope objective (a detailed description of the experimental setup is explained in the next section). The average cross-sectional plot of the beam profile is also shown in Fig. 3d.

We can sweep this fringe pattern across the illumination area by only changing the phase delay between the two beams, without physically scanning the illumination setup. The different phase delays will result in either destructive or constructive interference of the two illumination sources at different positions along the interface plane. A more detailed study of this effect is shown in Fig. S2 of the Supporting Information. Part (a) of Fig. S2 shows the cross-sectional field profile of the fringe pattern for phase delays of 0, 90, 180 and 270 degrees between the two illumination sources.

The illumination fringe pattern is also physically scanned across the gate layout to acquire the farfield image of the entire gate. We have decreased the physical scanning points required to cover the gate area by benefiting from the fringe pattern sweeping property for different phase delays, which allows us to obtain the gate's final image more rapidly. Another advantage of this sweeping property is finding the location of the nanoantenna and ensuring it is illuminated by the peaks of the fringe pattern.

In addition, we align the period of the fringe pattern by changing the sources' illumination angles. A more detailed study of this effect is shown in Fig. S2 of the Supporting Information. The cross-sectional field profile plot shown in Fig. S2, part (b) demonstrates the fringe pattern period variations by changing the illumination angles of two Gaussian sources to 30, 40, 50 and 60 degrees. This property is useful for choosing the appropriate illumination angle for reading out specific signatures from different gates that are built by different grating structures. We obtain the desired illumination fringe pattern period that matches the grating structure designed for our target gate's signature by changing the incident angle.

The position of the nanoantenna and the grating bars with respect to the illumination fringe pattern is very crucial and will significantly affect their farfield reflection response. Depending on the phase delay between the two sources, the grating bars and nanoantenna are located in the peaks or valleys of the fringe pattern. For a more detailed study of this effect please refer to Fig. S3 of the Supporting Information. Fig. S3(a) to (d) show the near electric field intensity pattern of our designed optical element, illuminated by the fringe pattern at different phase delays.

E. EXPERIMENTAL SETUP

Fig. 4a shows the experimental setup that we used to generate the illumination fringe pattern. An SLM and linear polarizer were used to apodize a larger Gaussian beam into two separate angled beams to generate the desired pattern for the initial experiment. The inset shows the SLM phase pattern applied in the experiment in order to obtain the fringe pattern. Fourier 4f lens pairs were used to propagate this pattern to the objective. The illumination diffraction pattern, shown in Fig. 3c, was obtained by magnifying the reflected beam and imaging the pattern with an InGaAs CCD camera. The hardware used in this initial method is limited to hundreds of Hz by the modulation speed of the SLM. So we propose a second method capable of GHz phase modulation. Our proposed high-frequency method consists of using a single coherent source split into separate optical fibers, then collimated into two beams. The phase delay between the two beams can be modulated at up to GHz speeds by using fiber

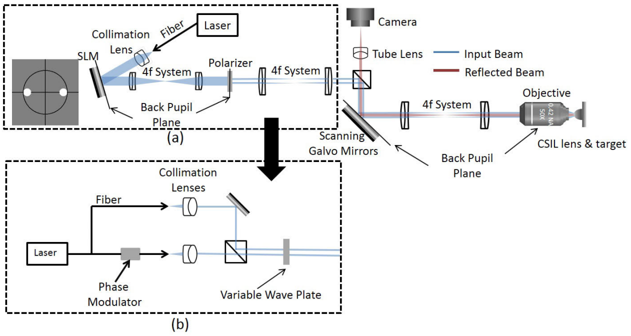

FIGURE 4. Experimental setup. (a) Implemented experimental setup: The SLM and the polarizer generate two separate beams which illuminate the sample through three 4f systems. The reflected light is recorded by the camera. (b) Proposed experimental setup, which uses two optical fibers to generate two separate beams. The phase modulator changes the phase delay between the two beams and allows high frequency sweeping of the diffraction pattern across the sample.

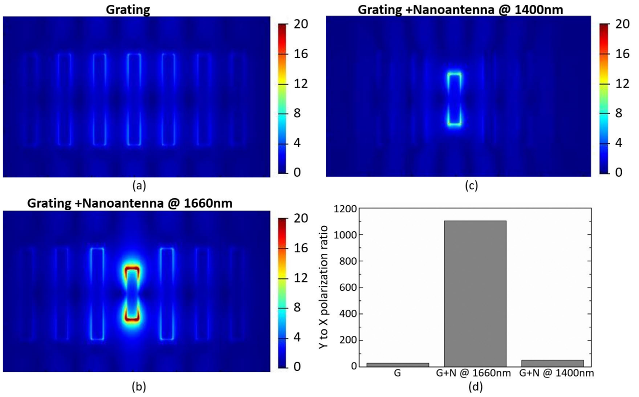

FIGURE 5. Simulations of near and far electric fields of three cases. (a) The grating structure (G) with dimensions comparable to the dimensions chosen for the optical signature grating. (b) The grating structure and nanoantenna illuminated at its LSPR wavelength of 1660 nm (G+N @ 1660 nm). (c) The grating structure and nanoantenna illuminated at 1400 nm (G+N @ 1400 nm). (d) The integrated farfield response ratio of longitudinally (Y) and transversely (X) polarized illumination for the three structures shown in a-c. In all simulations, the metal structures are embedded in SiO_2 medium, with a distance of 100 nm from the top surface of a silicon substrate, the same medium refractive index in the IC layout. The color bar values shown in parts a-c are in arbitrary units.

phase modulators. The second proposed experimental setup is shown in Fig. 4b.

After designing the illumination setup, we performed a series of simulations to investigate the effectiveness of our proposed optical signature. In order to do so, we compare the near and farfield reflection responses of two cases: a grating structure, and a grating plus nanoantenna in the center. Fig. 5a and 5b show the simulated near electric field pattern of these two cases in which both the nanoantenna and the grating structures are made of Copper, embedded in SiO_2 medium, and placed on top of the layered Si/SiO_2 substrate. The structures are illuminated by two Gaussian sources at the plasmonic resonance wavelength of the nanoantenna (1660 nm), with incident angles of 40 and −40 degree, which matches the periodicity of the fringe pattern with the periodicity of the grating structure. The phase delay between the two sources has been chosen such that all the grating bars and the nanoantenna are located at the peaks of the generated fringe pattern. The strong resonance around the nanoantenna in part b is 20× higher than the weak resonances around the grating bars in part a, verifying the effectiveness of the proposed optical signature.

Fig. 5c shows the near electric field pattern of the grating structure plus nanoantenna, when illuminated at the wavelength of 1400 nm, far from the plasmon resonance wavelength. We observe a much weaker resonance of the nanoantenna in this case, confirming the wavelength dependency of our proposed signature.

We also studied these three cases' farfield reflection patterns as shown in Fig. S4 of the Supporting Information, for both Y and X polarized illumination sources. In order to perform dark field measurement of these cases, we integrate the farfield reflection responses over the central 10-degree cone of angles for incident angles of 40 and −40 degrees.

Fig. 5d indicates a comparison of the farfield responses of the three cases presented in Fig. 5a-c. The y-axis in this plot indicates the intensity of the ratio of the farfield reflection integrated values, from the longitudinally polarized to transversely polarized illuminations. As expected, we observe the highest ratio for the case of a grating plus nanoantenna when illuminated at the plasmon resonance wavelength.

F. COLLECTION SETUP DESIGN

There are two crucial characteristics of a measurement technique which should be considered in order to determine the effectiveness and practicality of the method. Firstly, the rate of obtaining the required measurement is an essential factor in any application involving a detailed analysis of a large area. For example, as mentioned earlier, unlike the excellent spatial resolution offered by Transmission Electron Microscopy (TEM) for detailed visualization of the IC features, its time-consuming measurement method has prevented its functionality as an authentication technique for IC chips. Secondly, the signal to noise ratio (SNR) is another determining factor in evaluating the usefulness of a measurement technique. To optimize these essential characteristics in our proposed IC authentication technique, we employ a lock-in measurement method combined with the optical imaging setup. Fig. 6a schematically describes the steps performed in the lock-in measurement loop. The two inputs of the lock-in loop are called reference and measurement signal. In order to obtain the measurement signal from the optical setup, the scattered light from the IC's metal 1 layer is collected through the objective and integrated into one value, while sweeping the phase delays between the two illumination beams. The phase modulator in the optical setup allows us to rapidly sweep the phase delay at GHz frequency rate and collect the integrated reflection response for each phase delay. Therefore, we obtain the time-based measurement signal for the lock-in loop. Also, the reference signal for the lock-in

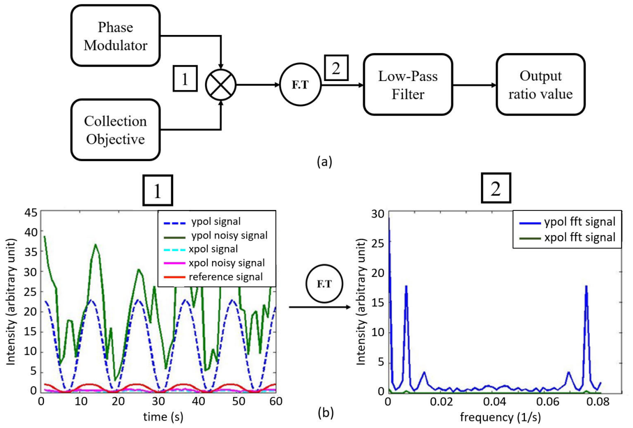

FIGURE 6. The lock-in measurement loop and the resulting response signals of a modified AND-NAND gate pair. (a) The lock in measurement method schematic: The measurement and reference signals are multiplied in time, then analyzed in frequency domain and finally passed through a low-pass filter. (b) The modified AND-NAND gate pair simulation results performed as a post processing step after FDTD simulations. Panel 1 shows the reference signal (red curve), measurement signals for both Y and X polarizations (dashed dark and light blue curves), and noisy measurement signals for both Y and X polarizations (green and pink curves). Panel 2 shows the frequency domain signals for both polarizations, after multiplying by the reference signal.

measurement is the carrier signal of the phase modulator. The reference and measurement signals are multiplied in the lock-in loop and converted to a frequency-based signal by Fast Fourier Transformation. Finally, the DC peak intensity of the resulting signal is extracted by passing it through a low-pass filter. We perform the same measurements for both Y and X polarized illuminations. The final output of the measurement is obtained by calculating the ratio of the DC intensity peaks of Y to X polarizations, which will be a single pixel in the final image of the chip. In order to image an IC chip, we will physically scan the illumination area (which is a circular region consisting of periodic fringes) over the entire chip by the scanning mirror. Therefore, the lock-in measurement methods allow us to rapidly acquire the IC's final image with a higher signal to noise ratio. We implement this lock-in detection setup as a MATLAB post-processing step in our simulations, where the lock-in measurement signal is extracted from the FDTD simulations of the chip for a set of phase delay sweeps for both polarizations.

Fig. 6b indicates a measurement signal extracted from FDTD simulations of a modified AND-NAND gate pair in order to be analyzed by our MATLAB algorithm for lock-in measurement method. The dashed dark and light blue curves in Plot 1 show the raw measurement signal for both Y and X polarized illuminations of the gate pair. These signals are achieved by recording the farfield reflection response of the gate for different phase delays between the two illumination beams. In order to simulate the noisy characteristics of the measurements in the experimental condition, we have added white Gaussian noise to the raw signals, shown with the green and pink curves, along with the red curve showing the reference signal. Plot 2 shows the frequency domain signal for Y and X polarizations, shown with blue and green curves respectively, after the Fourier transformation step shown in Fig. 6a. Finally, the next step is applying a low-pass filter to the signals, which will generate the intensity of the DC signal (intensity of the peak at zero frequency shown in the plot) for both polarizations. The ratio between these two intensities will generate the pixel intensity value, corresponding to the specific physical scanning point, in the final image of the gate pair.

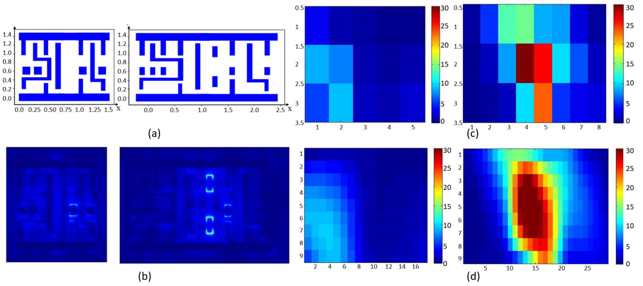

FIGURE 7. Comparison of original and modified AND-NAND gate pair reflection pattern. (a) Layout of the modified (right) and original (left) AND-NAND gate pair. The metal structures on the M1 (Metal 1) layer are shown as blue polygons in white background. (b) The simulated near electric field pattern of both gate pairs for Y polarization. The gate pair is illuminated by two angled Gaussian sources of 40 and −40 degree at the wavelength of 1350 nm, the LSPR of the designed nanoantenna. (c) The farfield optical image of both modified (right) and original (left) gate pair. (d) The interpolated farfield optical image of both modified and original gate pair with 0.25 times the pixel size in part c. The color bar values in parts c and d are unitless as they show the ratio of the logic gate's reflection intensity for Y and X polarization illuminations, after performing lock-in measurement.

III. RESULTS

A. COMPARISON OF THE ORIGINAL AND MODIFIED LOGIC GATE WITH EMBEDDED OPTICAL SIGNATURE

In this section, we evaluate the proposed optical imaging technique for IC authentication by embedding the optical elements shown in Fig. 1 in the layout of a gate pair. We design the modified gate pair layout such that the nanoantenna is placed in the empty space between two gates and the grating structure around the nanoantenna is built by modifying the existing periodic structures in the standard gate designs, resembling a grating. Fig. 7a shows the metal 1 layer layout of the original and modified AND-NAND gate pair, from left to right. In order to incorporate the nanoantenna in the design, we stretch the gate horizontally and then modify the width of periodic structures to match the design of the grating. After each modification, we use Design Rule Check (DRC) tool, Caliber, to make sure that the gate design does not violate any design rules. We design the optical signature parameters for this gate pair with a grating periodicity that matches the illumination fringe pattern periodicity corresponding to the illumination angles of 40 and −40 degrees and the nanoantenna size of 100 nm × 250 nm resulting in the LSPR wavelength of 1350 nm.

Fig. 7b shows the near electric field pattern of both original and modified gate pair when illuminated by two 40 and −40 degree angled Gaussian sources at the wavelength of 1350 nm for longitudinally polarized beams (along the long axis of the plasmonic nanoantenna). The high-intensity resonance around the nanoantenna, confirms a much stronger reflection response from the modified gate pair compared to the original gate pair.

We next implement the lock-in measurement method described in Fig. 6 to obtain the farfield optical image of the gate pair. To get the image of the whole gate pair we scan the illumination area over its layout. We choose the scanning steps in the X direction equal to the periodicity of the illumination fringe pattern. Depending on the illumination angle, the fringe period and therefore the scanning steps will change. However, the scanning step in the Y direction is constant since the length of all logic gates is equal to 1400 nm. We choose scanning step of 350 nm resulting in three scanning points of 350 nm, 0 nm and −350 nm. If we consider 0 nm scanning point (the center of the circular illumination area) to be at the center of the gate layout, these scanning steps will result in overlapping illumination areas covering the entire gate layout and therefore ensuring we are not undersampling the gate's response.

At each scanning step, the phase modulator changes the phase delay between the two illumination sources which will shift the fringe pattern with a maximum shift of half of the fringe period at the phase delay of 180 degrees (as shown in Fig. S2, Part b). We then analyze the measurement signal for Y and X polarization in the frequency domain. The resulting signal will pass through the low-pass filter, which will result in the DC peak intensity of the signals. The pixel value corresponding to this scanning point in the final image will be the ratio of the DC peak intensity of Y to X polarization signals. The same process is done for the next physical scanning point. Finally, all the pixel values corresponding to each scanning point are stitched together to obtain the final farfield optical image of the gate pair as shown in Fig. 7c. It is clearly observed that the modified gate pair (the right panel) generates a farfield reflection map containing high-intensity pixel values corresponding to the physical scanning points around the nanoantenna location in the gate pair layout. These high-intensity pixels show around 30× enhancement compared to the farfield image of the original gate pair (the left panel). Also, Fig. 7d indicates the interpolated farfield optical image of the same gate pairs with 0.25 times the pixel size in the original pixelated images, showing a smoother optical image of these gate pairs.

In order to show the wavelength dependency of the proposed optical signature, we simulated the modified AND-NAND gate pair response with different illumination setups, consisting of two angled illumination sources at 40 and −40 degrees, while changing the illumination wavelengths to 1150, 1350, 1540 and 1720 nm. These values correspond to the LSPR wavelength of all the chosen nanoantenna dimensions for different signatures, as shown in Fig. 2a. For simplicity, we run these simulations only for the most important scanning point, which is when the illumination fringe pattern is centered at the nanoantenna position in the gate pair layout, corresponding to the strongest pixel in reflection pattern in Fig. 7c right panel. We then conduct the lock-in measurement method by changing the phase delay between the two sources in order to get the final pixel value, for both X and Y polarizations. Fig. S5 indicates the intensity of this pixel value, the ratio of the DC peak intensity of Y to X polarization, for different illumination wavelengths and it clearly confirms that the highest intensity is obtained for 1350 nm wavelength, which matches the LSPR of the 100 nm × 250 nm nanoantenna embedded in this gate pair layout.

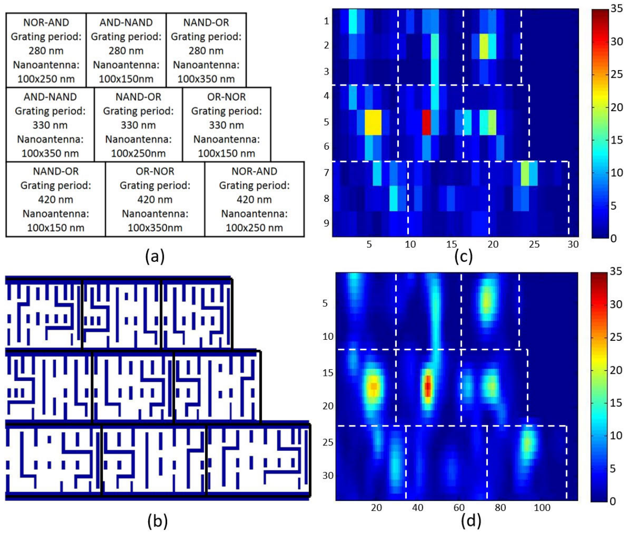

FIGURE 8. Evaluating the performance of the designed optical signature in a gate array. (a) The modified gate pairs, with their corresponding grating and nanoantenna, simulated in the gate array. (b) The metal 1 layer layout of the 3 × 6 array of logic gates. (c) Farfield heatmap of the gate array simulated in FDTD, by scanning the illumination area over the entire array. (d) The interpolated farfield optical image of gate array with 0.25 times the pixel size in part c. The color bar values in parts c and d are unitless as they show the ratio of the logic gate's reflection intensity for Y and X polarization illuminations, after performing lock-in measurement.

B. OPTICAL SIGNATURE PERFORMANCE EVALUATION IN LOGIC GATE ARRAY

We have shown the effectiveness of our optical signature in generating a distinct and strong farfield reflection map for an isolated gate pair when illuminated with the appropriate illumination setup. However, there are thousands of logic gates located next to each other in an actual IC chip. In order for the optical signature to function properly, the surrounding metal structures from the neighboring gates should not interfere with the response of the target gate.

We evaluate the performance of our proposed detection technique in an actual IC by simulating a 3 × 6 array of modified logic gates. Fig. 8a shows the modified gate pairs in the gate array, along with their corresponding grating periodicity and the incorporated nanoantenna dimension. Fig. 8b shows the modified layout of the metal 1 layer of the gate array. In the modified layout we have incorporated the nanoantenna and the grating structures between predetermined gate pairs. The target gate pair in this array is the modified NAND-OR gate pair located at the center of the array. The gate array is illuminated by two Gaussian sources at illumination angles 40 and −40 degrees and 1350 nm illumination wavelength, which match respectively, the grating periodicity and also the LSPR wavelength of the nanoantenna dimension incorporated in the target gate pair layout. In order to image the whole gate array, we should scan the illumination area over the entire array. The scanning steps in X direction equals the periodicity of the illumination fringe pattern which is 330 nm for 40-degree illumination angle. For each physical scanning point, the phase delay sweep between the sources and the lock-in measurement is performed to get the final pixel value. Once the pixel value for each scanning point is obtained, these values are stitched together to produce the final reflection pattern (resembling a heat map) of the gate array which is shown in Fig. 8c. Clearly, the highest intensity pixel is observed at the center of the target gate pair where the nanoantenna is placed. The weaker intensity pixels in the reflection pattern correspond to the place of the nanoantennas in neighboring gate pairs. The weaker intensity is due to the fact that either their nanoantenna LSPR or their grating periodicity doesn't match the illumination setup parameters.

Also, Fig. 8d indicates the interpolated farfield optical image of the same gate array with 0.25 times the pixel size in the original pixelated image. The edges of the designed gate pairs in the array are shown with dashed white lines in Fig. 8c and d. As observed in Fig. 8b, the width of each row in the gate array is different, which is both due to the gate pair's different widths in the original layout and also our different modifications applied to the layout of gate pairs for embedding various periodicity of gratings. For simplicity of data presentation, we have replaced the empty pixels at the end of each row in the final reflection pattern with zero values.

IV. DISCUSSION

In this study, we developed a fast and robust optical imaging technique to validate the authenticity of IC chips. Our method relies on creating watermarks in an IC based on the combination of its logic gates' optical signatures built from their specific farfield reflection pattern. We obtain these signatures by modifying the gate's metal 1 layer and integrating a combination of grating and a plasmonic nanoantenna in the gate layout. The gate's modified layout generates a strong, predetermined farfield reflection pattern for specific illumination parameters. The optical signatures are detected through a dark-field structured-illumination imaging setup allowing for detection of the sub-diffraction limited structures in the modified gate design. In order to read-out the watermarks efficiently and accurately, we combined the optical imaging setup with a lock-in measurement method which provides a rapid and accurate read-out of the gate's farfield response for two illumination polarizations through FFT. We achieved a 30× enhancement in the farfield reflection intensity of the modified gate layout compared to the original layout. In addition, we evaluated our proposed imaging technique in a gate array to investigate the effect of neighboring gates on the optical signature of the target gate pair. We successfully demonstrated that in a gate array, only the target gate pair lights up for its corresponding optimized illumination parameters.

We need to consider several parameters to determine the overall image acquisition speed of our IC authentication technique. The illumination spot size in our technique is on the order of a logic gate dimension (on average around $1\ \mu m \times 1 \mu$m) and with 2× oversampling the scan step size in confocal imaging will be on the order of 500 nm. An alternative method for gate authentication can be envisioned through direct imaging of the detailed structure of the metal 1 layer. In earlier studies, we have demonstrated subsurface confocal imaging with better than 150 nm resolution [31] that would allow a direct mapping of the metal structure and thus gate identification. However, this high-resolution direct imaging requires a scan step size of the order of 50 nm. Our new IC authentication method has nearly 100-fold speed increase over brute-force direct imaging. The integration time is another determining factor in acquisition speed, which depends on the SNR level. In our proposed technique, we have improved the SNR by 1) engineering the placement of the plasmonic nanoantenna so that we enhance the reflected signal, and 2) engineering the surrounding grating structures such that it matches the illumination fringe pattern periodicity so that we reduce the background light from other metal layers. The illumination spot is scanned using a galvo mirror (MHz acquisition rate) and at each scanning step, the fringe pattern is swept using a fiber phase modulator, which provides speeds up to GHz rate. So, same as a conventional confocal setup, our image acquisition speed is dependent on the galvo scanning speed. Therefore, to image a cm^2 area of an IC, we need to take 4×10^8 samples (with 500 nm scanning steps ensuring oversampling with our illumination spot size). Therefore, the image acquisition using our technique takes only a few minutes to cover the cm^2 area compared to standard confocal technique which could take anywhere from several hours to tens of days [32]. Please refer to section (Estimated Image Acquisition Time) in Supporting Information for a more detailed evaluation of our imaging speed and comparison with the standard confocal imaging.

In this study, we have also shown the robustness of our proposed technique to background noise and process variation. The enhanced SNR achieved in our technique, by matching the illumination fringe pattern to the embedded grating structures, improves the robustness of the imaging system to the background noise. In addition, we also demonstrated the robustness of the system to process variations. To do this, we determined the uniqueness of the signatures of different nanoantenna dimensions resulting from process variations applied to the originally designed nanoantenna dimensions.

As the future direction of this study, we are currently also working on fabricating these designed logic gates as well as building and optimizing the optical setup for imaging. In addition, we propose adding the gate identification capability to our technique using machine learning algorithms. In order to train the classification algorithm, we generate the training data set by collecting all the modified gate pair's images from different combinations of illumination setups (illumination angles and illumination wavelengths). Basically, in addition to the optimized illumination parameters for each modified gate pair, its response to all the other illumination settings is also obtained. All these responses will be saved in a feature vector, acting as a fingerprint for each gate pair in our training phase. It is worth mentioning that even if we employ the same optical structures in various gate pairs, their farfield reflection responses will be slightly different because of the different surrounding metal structures in the gates' layout. With the help of machine learning, the pre-trained models could classify a measured test gate by comparing its feature vectors to the library of feature vectors developed in the training phase. The potential classification methods are K-Nearest-Neighbors, Support Vector Machines and Random Forest. With the help of machine learning, the pre-trained models classify the feature vectors for labeling the measured test gate. In previous work [32], we applied classifier algorithms in order to identify different gates based on multispectral imaging of the original gate layout. The limitations of the previous study arise from working with the weak reflection images of the original gate's layout as the training data set. However, in the current study, the classification capability of the algorithm will be significantly improved due to using the reflection response of the modified gate layout as the training data set. The modifications applied to the gate physical layout generate a much stronger and distinct reflection pattern for each gate pair, therefore improving the certainty of the gate identification based on the pre-trained model.

V. PROPOSED APPLICATIONS

Our proposed IC authentication method provides a nondestructive, rapid and robust inspection of ICs for detecting HTs inserted during the manufacturing stage and also counterfeit IC chips detection.

Counterfeiting IC chips is a very common problem, where a malicious person uses low-grade IP blocks or low-grade dies and sells them as high-grade, well-branded products to make a quick profit [12]. To prevent this malicious use of the IP blocks and dies, an efficient and low-cost method is required to identify their authenticity. Previously, Chakraborty and others have proposed the use of logic obfuscation to prevent IC counterfeiting through over-building [9]. Their technique works such that the logic of the IP block is locked until the trusted third-party providing the correct sequence can unlock the IP block. To detect the authenticity of the IP block in the fabricated ICs or the die, we propose to use optical imaging. In the post-silicon authentication step, we can detect which IP blocks have been used or which die has been used by backside imaging. If the IP block or die is different than what it should be then it will get detected through backside imaging and we can flag the IC chip as counterfeit.

Hardware Trojans are malicious designs inserted into IC chips that can damage or disrupt the intended functionality of a device or be used to leak sensitive information to an adversary in future [33]. We focus on HTs 1) inserted in the form of a new structure (such as A2 [8] where the HT is a logic gate) in the physical layout of the IC, or 2) inserted by modifying the layout of the logic gates. Previous HT detection methods, such as power and timing tests [34], cannot reliably detect these HTs due to their sizes and triggering rate. In fact, in recently published works, several researchers have designed HTs that are as small as one gate [5, 8]. This single-gate HT is extremely hard, if not impossible, to detect. The attacker can design the HT to have an extreme low triggering rate which can bypass all the IC testing, such that only the attacker can launch attack [8]. We use optical imaging technique to image the physical layout of the design and detect the HT. Our technique is independent of the HT size and does not require triggering of the HT.

Here is how our proposed method could be employed to detect the HTs:

1) *Hardware Trojans inserted in the form of a new structure in the IC layout:* The basis of our IC authentication technique is obtaining the expected reflection pattern from the IC layout. This reflection pattern resembles a heat map that consists of bright spots at specific locations corresponding to the logic gates that were designed to light up for a specific illumination parameter set. (refer to Figure 8)

If during the IC fabrication step, an adversary party inserts a new structure, even as small as a logic gate, in the IC layout, this will result in moving the other logic gates in the IC and therefore changing the expected location of the bright spots in the IC farfield reflection pattern. So by comparing the obtained reflection pattern to our IC's expected reflection pattern, we could detect any mismatch in the location of the bright spots. A mismatch in the bright spots would indicate the insertion of an HT.

2) *Logic gate layout is modified such that the gate behaves as an HT:* Our method proposes to design a unique optical signature for each logic gate. This is achieved by engineering the physical layout of each logic gate. If the adversary party uses a logic gate (for inserting the HT) that is not engineered to resonate at a specific illumination parameter set, we will be able to detect this logic gate as it won't light up in the reflection map of the IC once it is illuminated by the appropriate illumination parameter sets.

It is worth mentioning that our method would fail to detect an HT if the intruder is familiar with the design and purpose of the embedded plasmonic nanoantenna and grating in the logic gate layout. In that case, the intruder could replace or modify a logic gate in the IC such that the plasmonic nanoantenna and grating structure embedded in the new/modified logic gate will still resonate at the appropriate illumination parameter set. Such an HT will go undetected. However, even if the intruder is familiar with our design parameters, he/she would still need to design his/her intended logic gate around our embedded optical elements, which adds a significant amount of difficulty to their design process. Therefore, in such cases our method essentially makes it harder for the intruder to insert an HT without going undetected.

VI. CONCLUSION

In this paper we propose an IC authentication method based on rapid and non-destructive optical imaging of embedded watermarks in metal 1 layer of the IC design. The optical watermarks are predetermined farfield reflection patterns for an IC. These patterns are achieved by modifying the design of the logic gates (that form the IC) to embed a plasmonic nanoantenna and grating structures in the gate layout. We read-out the embedded watermarks using a dark-field structured-illumination imaging technique combined with lock-in signal acquisition. Through our designed logic gate layout modification, we achieve 30× enhancement in the polarization-dependent farfield reflection intensity signal. Our proposed IC authentication can be used for detecting counterfeit IC chips as well as HTs inserted during the manufacturing stage of IC chips.

ACKNOWLEDGMENT

The authors would like to thank Ronen Adato, Aydan Uyar and Bennett Goldberg for their contribution in the early development of this study.

REFERENCES

[1] "60 years of integrated circuits," *Nature Electron.*, vol. 1, p. 483, Sep. 2018, Editorial, doi: 10.1038/s41928-018-0145-6.

[2] J. S. Kilby, "Invention of the integrated circuit," *IEEE Trans. Electron Devices*, vol. 23, no. 7, pp. 648–654, Jul. 1976.

[3] V. Venugopalan and C. D. Patterson, "Surveying the hardware trojan threat landscape for the Internet-of-Things," *J. Hardw. Syst. Secur.*, vol. 2, no. 2, pp. 131–141, Jun. 2018.

[4] D. Jones. (Sep. 2018). *The Power of Transistor Density: A Look at AMD, Intel, and How Moore's Law is Affecting the Market*. [Online]. Available: https://www.allaboutcircuits.com/news/power-of-transistor-density-amd-intel-how-engineering-affects-the-market

[5] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 27, no. 1, pp. 10–25, Jan./Feb. 2013.

[6] P. Aryan, S. Sampath, and H. Sohn, "An overview of non-destructive testing methods for integrated circuit packaging inspection," *Sensors*, vol. 18, no. 7, p. 1981, 2018.

[7] G. Tessier, M. Bardoux, C. Filloy, C. Boué, and D. Fournier, "High resolution thermal imaging inside integrated circuits," *Sensor Rev.*, vol. 27, no. 4, pp. 291–297, Sep. 2007.

[8] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog malicious hardware," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 18–37.

[9] S. Wei, S. Meguerdichian, and M. Potkonjak, "Gate-level characterization: Foundations and hardware security applications," in *Proc. 47th Design Autom. Conf. (DAC)*, Jul. 2010, pp. 222–227.

[10] P. Song, F. Stellari, D. Pfeiffer, J. Culp, A. Weger, and A. Bonnoit, "MARVEL—Malicious alteration recognition and verification by emission of light," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust*, Jul. 2011, pp. 117–121.

[11] F. Stellari, P. Song, and H. A. Ainspan, "Functional block extraction for hardware security detection using time-integrated and time-resolved emission measurements," in *Proc. IEEE 32nd VLSI Test Symp. (VTS)*, Napa, CA, USA, Apr. 2014, pp. 1–6, doi: 10.1109/VTS.2014.6818792.

[12] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.

[13] M. C. Hansen, H. Yalcin, and J. P. Hayes, "Unveiling the ISCAS-85 benchmarks: A case study in reverse engineering," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 16, no. 3, pp. 72–80, 3rd Quart., 1999.

[14] H. Stegmann, H.-J. Engelmann, and E. Zschech, "Transmission electron microscopy in semiconductor manufacturing," in *Science, Technology and Education of Microscopy: An Overview*. Des Moines, LA, USA: Formatex, 2003, pp. 187–199.

[15] R. Adato, A. Joshi, M. S. Unlu, and B. B. Goldberg, "Gate-level mapping of Integrated Circuits using multi-spectral imaging," U.S. Patent 10 282 833, May 7, 2019.

[16] B. Zhou, R. Adato, M. Zangeneh, T. Yang, A. Uyar, B. Goldberg, S. Unlu, and A. Joshi, "Detecting hardware trojans using backside optical imaging of embedded watermarks," in *Proc. 52nd Annu. Design Autom. Conf. (DAC)*, San Francisco, CA, USA, Jul. 2015, pp. 1–6.

[17] R. Adato, A. Uyar, M. Zangeneh, B. Zhou, A. Joshi, B. B. Goldberg, and M. S. Ünlü, "Integrated nanoantenna labels for rapid security testing of semiconductor circuits," in *Proc. Frontiers Opt.*, San Jose, CA, USA, 2015, Art. no. FTh1B.2.

[18] J. L. Saint and C. Saint. (2018). *Integrated Circuit*. [Online]. Available: https://www.britannica.com/technology/integrated-circuit

[19] R. Pappu, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[20] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[21] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging physical unclonable functions with nanotechnology," *IEEE Access*, vol. 4, pp. 61–80, 2016.

[22] W. Spitzer and H. Y. Fan, "Infrared absorption in n-type silicon," *Phys. Rev.*, vol. 108, pp. 268–271, Oct. 1957.

[23] A. Stillmaker and B. Baas, "Scaling equations for the accurate prediction of CMOS device performance from 180 nm to 7 nm," *Integration*, vol. 58, pp. 74–81, Jun. 2017.

[24] K. L. Kelly, E. Coronado, L. L. Zhao, and G. C. Schatz, "The optical properties of metal nanoparticles: The influence of size, shape, and dielectric environment," *J. Phys. Chem. B*, vol. 107, pp. 668–677, Jan. 2003.

[25] V. Juvé, M. F. Cardinal, A. Lombardi, A. Crut, P. Maioli, J. Pérez-Juste, L. M. Liz-Marzán, N. Del Fatti, and F. Vallée, "Size-dependent surface plasmon resonance broadening in nonspherical nanoparticles: Single gold nanorods," *Nano Lett.*, vol. 13, no. 5, pp. 2234–2240, May 2013.

[26] M. A. El-Sayed, "Some interesting properties of metals confined in time and nanometer space of different shapes," *Accounts Chem. Res.*, vol. 34, no. 4, pp. 257–264, Apr. 2001.

[27] M. M. Shahjamali, Y. Zhou, N. Zaraee, C. Xue, J. Wu, and N. Large, "Ag–Ag$_2$S hybrid nanoprisms: Structural versus plasmonic evolution," *ACS Nano*, vol. 10, pp. 5362–5373, May 2016.

[28] M. M. Shahjamali, M. Bosman, S. Cao, X. Huang, S. Saadat, E. Martinsson, D. Aili, Y. Y. Tay, B. Liedberg, S. C. J. Loo, H. Zhang, F. Boey, and C. Xue, "Gold coating of silver nanoprisms," *Adv. Funct. Mater.*, vol. 22, no. 4, pp. 849–854, Feb. 2012.

[29] S. Mittal, "A survey of architectural techniques for managing process variation," *ACM Comput. Surveys*, vol. 48, no. 4, pp. 1–29, May 2016.

[30] C. Palmer, *Diffraction Grating Handbook*, 7th ed. Rochester, NY, USA: Richardson Gratings, Feb. 2014.

[31] F. H. Köklü, S. B. Ippolito, B. B. Goldberg, and M. S. Ünlü, "Subsurface microscopy of integrated circuits with angular spectrum and polarization control," *Opt. Lett.*, vol. 34, no. 8, pp. 1261–1263, Apr. 2009.

[32] R. Adato, A. Uyar, M. Zangeneh, B. Zhou, A. Joshi, B. Goldberg, and M. S. Unlu, "Rapid mapping of digital integrated circuit logic gates via multi-spectral backside imaging," 2016, *arXiv:1605.09306*. [Online]. Available: http://arxiv.org/abs/1605.09306

[33] J. Vosatka, *Introduction to Hardware Trojans in the Hardware Trojan War: Attacks, Myths, and Defenses*. Cham, Switzerland: Springer, 2018, pp. 15–51.

[34] A. Nejat, D. Hely, and V. Beroulle, "Facilitating side channel analysis by obfuscation for hardware trojan detection," in *Proc. 10th Int. Design Test Symp. (IDT)*, Amman, Jordan, Dec. 2015, pp. 129–134.

NEGIN ZARAEE (Student Member, IEEE) received the B.S. degree in electrical engineering from Shiraz University, Shiraz, Iran, in 2012. She is currently pursuing the Ph.D. degree in electrical engineering with the Optical Characterization and Nanophotonics Laboratory, Boston University, Boston, MA, USA.

Her research interests include applications of nanophotonics in integrated circuits authentication, as well as design and development of optical biosensors. Her current researches focus on designing interferometric biosensors for rapid, sensitive and multiplexed bacteria detection, as well as the bacterial antibiotic resistivity studies.

BOYOU ZHOU received the B.S. degree in computer engineering from Southeast University, China, and the Ph.D. degree in hardware security from Electrical and Computer Engineering Department, Boston University, Boston, MA, USA, in 2019.

He is currently working with Analog Garage, Analog Devices Inc. His research interests include hardware designs in security and hardware assisted software security. He has also worked as an intern in Real Number Modeling in Analog Devices Inc.

KYLE VIGIL received the B.S. degree in physics and mathematics from Texas A&M University, College Station, Texas, in 2006, the master's degree in physics from Boston University, Boston, Massachusetts, in 2015. He served as a Communications Officer in the United States Marine Corps, from 2006 to 2010.

MOHAMMAD M. SHAHJAMALI received the Ph.D. and B.S. degrees in material science and engineering with Nanyang Technological University and Shiraz University. He has worked intensively on novel synthesis, optical properties and applications of anisotropic plasmonic silver, gold and platinum nanostructures. He worked as a Postdoctoral Researcher on DNA-mediated self-assembly of anisotropic nanostructures for photonics and plasmonic applications and he has hands-on experience on optical properties of metal-semiconductor nanoparticles with the International Institute for Nanotechnology, Northwestern University. He is currently a Research Associate with Harvard University working on Self-Assembly of filamentous nanowires into nanotwist, nanobraid and nanocoil topologies with applications in nanoelectronics and NEMS industries.

AJAY JOSHI (Senior Member, IEEE) was born in Mumbai, India. He received the Ph.D. degree from the ECE Department, Georgia Technology, in 2006. He worked as a Postdoctoral Researcher with the EECS Department, MIT. In 2009, he joined the ECE Department with Boston University, where he is currently an Associate Professor. He was a Visiting Researcher with Google, from 2017 to 2018. His research interests span across various aspects of VLSI design including circuits and architectures for communication and computation. He received the NSF CAREER Award, in 2012, Boston University, ECE Department's Award for Excellence in Teaching, in 2014, Google Faculty Research Award 2018 and 2019, and Best Paper Award at ASIACCS 2018. He currently serves as the Associate Editor for the IEEE Transactions on VLSI Systems.

M. SELIM ÜNLÜ (Fellow, IEEE) received the B.S. degree from the Middle East Technical University, Ankara, Turkey, in 1986, and the M.S.E.E. and Ph.D. degrees from the University of Illinois at Urbana–Champaign, all in electrical engineering, in 1988 and 1992, respectively.

Since 1992, he has been on the Faculty of Boston University, currently appointed as a Distinguished Professor of Engineering. He is appointed in electrical and computer engineering and affiliated with biomedical engineering, physics, material science and engineering, and graduate medical sciences. He has served as the Associate Dean for Research and Graduate Programs in engineering as well as the Associate Director of Center for Nanoscience and Nanobiotechnology. His research interests are in the areas of nanophotonics and biophotonics focusing on high-resolution solid immersion lens microscopy of integrated circuits and development of biological detection and imaging techniques, particularly in multiplexed detection of single viral pathogens and protein and nucleic acid microarrays.

Dr. Ünlü was the recipient of the National Science Foundation CAREER and Office of Naval Research Young Investigator Awards in 1996. He has been selected as a Photonics Society Distinguished Lecturer for 2005–2007 and Australian Research Council Nanotechnology Network (ARCNN) Distinguished Lecturer for 2007. He has been elevated to IEEE Fellow rank in 2007 for his contributions to optoelectronic devices and OSA Fellow rank in 2017 for his for pioneering contributions in utilization of optical interference in enhanced photodetectors and biological sensing and imaging. In 2008, he was awarded the Science Award by the Turkish Scientific Foundation. His professional service includes the former chair of photodetectors and imaging, and biophotonics, and founding Chair of Nanophotonics Technical Committees for the IEEE Photonics Society, and Editor-in-Chief for the IEEE Journal of Quantum Electronics.