3-27-2015

Uniquely Identifiable Tamper-Evident Device Using Coupling between Subwavelength Gratings

Ange Marie P. Fievre
Florida International University, pfiev001@fiu.edu

DOI: 10.25148/etd.FI15032173
Follow this and additional works at: https://digitalcommons.fiu.edu/etd

Part of the Electromagnetics and Photonics Commons, and the Nanotechnology Fabrication Commons

Recommended Citation
https://digitalcommons.fiu.edu/etd/1762

This work is brought to you for free and open access by the University Graduate School at FIU Digital Commons. It has been accepted for inclusion in FIU Electronic Theses and Dissertations by an authorized administrator of FIU Digital Commons. For more information, please contact dcc@fiu.edu.
FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

UNIQUELY IDENTIFIABLE TAMPER-EVIDENT DEVICE USING COUPLING BETWEEN SUBWAVELENGTH GRATINGS

A dissertation submitted in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY in ELECTRICAL ENGINEERING by Ange Marie Patricia Fievre

2015
To: Dean Amir Mirmiran  
College of Engineering and Computing

This dissertation, written by Ange Marie Patricia Fievre, and entitled Uniquely Identifiable Tamper-Evident Device Using Coupling Between Subwavelength Gratings, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

_______________________________________  
Al-Aakhir Rogers

_______________________________________  
Irene Calizo

_______________________________________  
Sakhrat Khizroev

_______________________________________  
William Kinzy Jones

_______________________________________  
Subramanian Krishnan

_______________________________________  
Roberto Panepucci

_______________________________________  
Shekhar Bhansali, Major Professor

Date of Defense: March 27, 2015

The dissertation of Ange Marie Patricia Fievre is approved.

_______________________________________  
Dean Amir Mirmiran  
College of Engineering and Computing

_______________________________________  
Dean Lakshmi N. Reddi  
University Graduate School

Florida International University, 2015
ACKNOWLEDGMENTS

This work was supported in part by the Florida Education Fund and by the National Science Foundation through the Nanosystems Engineering Research Center (NERC) for Advanced Self-Powered Systems for Integrated Sensors and Technology (ASSIST), under grant ERC-1160483.
ABSTRACT OF THE DISSERTATION

UNIQUELY IDENTIFIABLE TAMPER-EVIDENT DEVICE USING COUPLING BETWEEN SUBWAVELENGTH GRATINGS

by

Ange Marie Patricia Fievre

Florida International University, 2015

Miami, Florida

Professor Shekhar Bhansali, Major Professor

Reliability and sensitive information protection are critical aspects of integrated circuits. A novel technique using near-field evanescent wave coupling from two subwavelength gratings (SWGs), with the input laser source delivered through an optical fiber is presented for tamper evidence of electronic components. The first grating of the pair of coupled subwavelength gratings (CSWGs) was milled directly on the output facet of the silica fiber using focused ion beam (FIB) etching. The second grating was patterned using e-beam lithography and etched into a glass substrate using reactive ion etching (RIE). The slightest intrusion attempt would separate the CSWGs and eliminate near-field coupling between the gratings. Tampering, therefore, would become evident.

Computer simulations guided the design for optimal operation of the security solution. The physical dimensions of the SWGs, i.e. period and thickness, were optimized, for a 650 nm illuminating wavelength. The optimal dimensions resulted in a 560 nm grating period for the first grating etched in the silica optical fiber and 420 nm for the second grating etched in borosilicate glass. The incident light beam had a half-width at half-maximum (HWHM) of at least 7 µm to allow discernible higher transmission
orders, and a HWHM of 28 µm for minimum noise. The minimum number of individual grating lines present on the optical fiber facet was identified as 15 lines. Grating rotation due to the cylindrical geometry of the fiber resulted in a rotation of the far-field pattern, corresponding to the rotation angle of moiré fringes. With the goal of later adding authentication to tamper evidence, the concept of CSWGs signature was also modeled by introducing random and planned variations in the glass grating.

The fiber was placed on a stage supported by a nanomanipulator, which permitted three-dimensional displacement while maintaining the fiber tip normal to the surface of the glass substrate. A 650 nm diode laser was fixed to a translation mount that transmitted the light source through the optical fiber, and the output intensity was measured using a silicon photodiode. The evanescent wave coupling output results for the CSWGs were measured and compared to the simulation results.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CHAPTER I: Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>1.1 Overview of Diffraction, Subwavelength and Coupled Gratings</td>
<td>1</td>
</tr>
<tr>
<td>1.1.1 Diffraction Gratings</td>
<td>1</td>
</tr>
<tr>
<td>1.1.2 Subwavelength Gratings</td>
<td>2</td>
</tr>
<tr>
<td>1.1.3 Coupled Gratings</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Research Purpose</td>
<td>4</td>
</tr>
<tr>
<td>1.3 Dissertation Organization</td>
<td>7</td>
</tr>
<tr>
<td><strong>CHAPTER II: Background and Motivation</strong></td>
<td>8</td>
</tr>
<tr>
<td>2.1 Background on Optical Fibers</td>
<td>8</td>
</tr>
<tr>
<td>2.1.1 Dielectric Waveguides</td>
<td>8</td>
</tr>
<tr>
<td>2.1.2 Step-Index Optical Fibers</td>
<td>22</td>
</tr>
<tr>
<td>2.2 The Necessity for IC Security</td>
<td>26</td>
</tr>
<tr>
<td>2.2.1 Types of Attacks</td>
<td>29</td>
</tr>
<tr>
<td>2.2.2 Classification of IC Security Solutions</td>
<td>34</td>
</tr>
<tr>
<td>2.2.3 IC Security Techniques</td>
<td>38</td>
</tr>
<tr>
<td>2.2.4 Integrity Solutions for Systems On a Chip</td>
<td>53</td>
</tr>
<tr>
<td><strong>CHAPTER III: Methodology</strong></td>
<td>56</td>
</tr>
<tr>
<td>3.1 Optical Simulations with Finite Difference Time Domain (FDTD)</td>
<td>57</td>
</tr>
<tr>
<td>3.2 Wavelength and Components Choice</td>
<td>62</td>
</tr>
<tr>
<td>3.3 Fabrication Methods</td>
<td>62</td>
</tr>
<tr>
<td>3.3.1 Electron Beam Lithography (EBL)</td>
<td>62</td>
</tr>
<tr>
<td>3.3.2 Focused Ion Beam (FIB) milling</td>
<td>64</td>
</tr>
<tr>
<td>3.3.3 Charging</td>
<td>64</td>
</tr>
<tr>
<td>3.4 Test Procedure</td>
<td>65</td>
</tr>
<tr>
<td><strong>CHAPTER IV: Simulation Results</strong></td>
<td>66</td>
</tr>
<tr>
<td>4.1 Simulation Set-Up</td>
<td>66</td>
</tr>
<tr>
<td>4.2 Optimization of Gratings Periods and Thicknesses</td>
<td>69</td>
</tr>
<tr>
<td>4.3 Effect of Beam Width</td>
<td>72</td>
</tr>
<tr>
<td>4.4 Effect of the Number of Grating Lines</td>
<td>74</td>
</tr>
<tr>
<td>4.5 Effect of Rotational Misalignment</td>
<td>76</td>
</tr>
<tr>
<td>4.6 Variations in Glass Grating</td>
<td>80</td>
</tr>
<tr>
<td>4.7 Conclusion</td>
<td>85</td>
</tr>
<tr>
<td><strong>CHAPTER V: Gratings Fabrication</strong></td>
<td>86</td>
</tr>
<tr>
<td>5.1 Gratings on Fiber Facet</td>
<td>86</td>
</tr>
<tr>
<td>5.2 Gratings on Glass Substrate</td>
<td>88</td>
</tr>
</tbody>
</table>
CHAPTER VI: Tests, Results and Discussion ................................................................. 94
  6.1 Test Set-Up ............................................................................................................. 94
    6.1.1 Light Sources ................................................................................................. 95
    6.1.2 Fiber and glass substrate mounting ............................................................... 96
    6.1.3 Readout ........................................................................................................... 97
  6.2 Testing .................................................................................................................. 97
    6.2.1 Gratings alignment ....................................................................................... 97
    6.2.2 Tests with large gratings ............................................................................. 100
    6.2.3 Evanescent coupling .................................................................................... 101
  6.3 Modeling and Measurements Comparison ........................................................... 104
  6.4 Conclusions and Future Work ............................................................................. 107

References ....................................................................................................................... 109

VITA ....................................................................................................................................... 131
<table>
<thead>
<tr>
<th>TABLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1: Comparison of the Main Four Types of Integrated Circuit Attacks</td>
<td>33</td>
</tr>
<tr>
<td>Table 2: Recapitulation of the FIPS physical security requisites. ([75])</td>
<td>35</td>
</tr>
<tr>
<td>Table 3: Summary of Security Solutions</td>
<td>53</td>
</tr>
<tr>
<td>Table 4: First order far-field output intensities of variable grating thicknesses for $\Lambda_1 = 560 \text{ nm} - \Lambda_2 = 420 \text{ nm}$ SWG pair</td>
<td>72</td>
</tr>
<tr>
<td>Table 5: Fringe angle, period and diffraction angle for different fiber rotation angles</td>
<td>79</td>
</tr>
<tr>
<td>Table 6: Parameters for FIB milling on fiber facets</td>
<td>87</td>
</tr>
<tr>
<td>Table 7: Output intensity in diffraction orders captured by photodetector with 560 nm – 420 nm grating pair</td>
<td>103</td>
</tr>
<tr>
<td>Table 8: Output intensity in diffraction orders captured by photodetector with 560 nm – 480 nm grating pair</td>
<td>104</td>
</tr>
<tr>
<td>FIGURE</td>
<td>PAGE</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
</tr>
<tr>
<td>Figure 1: Total geometrical path difference between light from adjacent grooves in a transmission grating</td>
<td>2</td>
</tr>
<tr>
<td>Figure 2: a): Plane wave source incident on coupled SWGs. Higher diffraction orders are exhibited at the output. b) Bonded pair of subwavelength gratings. c) Simulation of CSWGs. d) simulated far-field output intensity of the first diffraction order for different gaps between the gratings [15]</td>
<td>3</td>
</tr>
<tr>
<td>Figure 3: a) In-package implementation of CSWGs chip security system. b) On-chip implementation of the system</td>
<td>5</td>
</tr>
<tr>
<td>Figure 4: Two instances of varied CSWGs generate two different signatures, while the first and second diffraction order are clearly visible</td>
<td>6</td>
</tr>
<tr>
<td>Figure 5: The slab waveguide, two-dimensional waveguide. The y-dimension extends to infinity</td>
<td>8</td>
</tr>
<tr>
<td>Figure 6: Case of light transmitted from a denser to a less dense medium, when $\theta_1 &lt; \theta_c$. The refracted ray in the low index medium leaves at an angle $\theta_2$</td>
<td>9</td>
</tr>
<tr>
<td>Figure 7: In a waveguide, light is launched so that $\theta_1$ exceeds the critical angle, and total internal reflection imprisons the ray inside the core</td>
<td>10</td>
</tr>
<tr>
<td>Figure 8: The evanescent wave travels along the separating surface, parallel to the waveguide</td>
<td>10</td>
</tr>
<tr>
<td>Figure 9: Discontinuity in material properties. When the properties of the material changes suddenly, $\bar{\mathbf{E}}, \bar{\mathbf{H}}, \bar{\mathbf{B}}, \bar{\mathbf{D}}$ must comply with a certain number of boundary conditions: continuity of the tangential components of the electric and magnetic fields, continuity of normal components of the electric and magnetic fluxes</td>
<td>13</td>
</tr>
<tr>
<td>Figure 10: The modes can be categorized in terms of Transverse Electric field (TE) and Transverse Magnetic field (TM). The TE field is perpendicular to the plane of incidence containing the normal to the interface and the k vector. In the TM case, the electric field is parallel to the plane of incidence</td>
<td>14</td>
</tr>
<tr>
<td>Figure 11: The geometric relation between $\beta$, $\kappa$ and k. $\beta$ is the propagation coefficient along the direction of propagation of the electromagnetic wave, which we chose to be z, and $\kappa$ is the transverse propagation constant</td>
<td>15</td>
</tr>
</tbody>
</table>
Figure 12: Light rays traveling inside a slab waveguide. For the propagation to continue, the interference between the rays must be constructive ...............16

Figure 13: The TE electric field patterns of the first three modes. The values of $\beta$ that satisfy the eigenvalues equations specify a discrete series of guided modes, alternatively symmetric and antisymmetric [21] .........................21

Figure 14: Layers of a typical optical fiber: higher-index core, lower-index cladding and external coating ........................................................................................................22

Figure 15: The projection of a skew ray on a plane perpendicular to the fiber axis forms a regular polygon ........................................................................................................23

Figure 16: Intensity plot for the first six LP modes in an optical fiber [23]. LP01 is from HE11, LP0m is from HE1m, LP1m is the sum of TE0m, TM0m, and HE2m, and LPnm is the sum of HEn+1,m and E Hn-1,m .........................24

Figure 17: Acceptance cone of an optical fiber ..................................................................25

Figure 18: Number of suspect counterfeit electronic parts for the period 2001 to 2012, most of them reported by military and aerospace firms in the U.S. Source: IHS Parts Management ........................................................................27

Figure 19: Side-channel attacks use information leaked during system operation. The input, the output and the side channel information are combined to recover the secret information or key. Side-channel information can be included in the power consumption, timing, or electromagnetic emission of the device during the processing of secret information .......................31

Figure 20: Security classification based on location and goal of the protection ...............37

Figure 21: Example of the use of tiling for fingerprinting, with the Boolean function Out = $(A \cap B) \cap (CUD)$. Since the function as well as the tile interface with adjacent design components are unchanging, the configurations shown are transposable ........................................................................42

Figure 22: In each integrated circuit, an array of devices produces a difference voltage sequence because of device mismatch. ICID uses these sequences of random but repeatable voltages to create unique identifications. ([118] © 2000 IEEE) ........................................................................................................43

Figure 23: A basic parallel delay-based PUF is shown. The path segments are designed to have the same delay but manufacturing variations cause the delays to differ slightly. The rising edge goes through the two different paths and the one-bit output is determined by which path allows the rising edge to arrive faster .........................................................44
Figure 24: Architecture of the ROPUF .................................................................45

Figure 25: Graphic cross-section of a Coating PUF IC. Aluminum sensors in the higher metal layer measure the local capacitance of the coating .......................52

Figure 26: Schematic of the coupled subwavelength grating setup. Source: A.-A. Rogers, "Evanescent wave coupling using subwavelength gratings for optical MEMS accelerometer," PhD Dissertation, Electrical Engineering, University of South Florida, Tampa, FL, 2011 .......................................................54

Figure 27: 3D design of fiber grating coupled with glass grating, and longitudinal cross-section of design in x-z plane .................................................................57

Figure 28: Standard Yee cell. The six field components are separated to each other by half a space step .........................................................................................59

Figure 29: Steps of resist patterning in typical EBL process .....................................63

Figure 30: Simulation setup .......................................................................................67

Figure 31: a) Coupled 200 nm and 500 nm gratings, with 1 µm equivalent period. b) Diffraction orders generated by coupled gratings when $\Lambda_1 = 200$ nm and $\Lambda_2$ is varied between 200 and 600 nm. In this case only the 200 nm - 500 nm pair is not subwavelength and gives rise to a diffraction order at about 40.5° ........................................................................................................68

Figure 32: Far-field peak intensities for different combinations of periods in coupled gratings ..........................................................................................................70

Figure 33: 1.68 µm equivalent grating period from a 560 nm and 420 nm grating pair ...................................................................................................................71

Figure 34: Effect of Beam Width on CSWGs with grating periods $\Lambda_1 = 560$ nm and $\Lambda_2 = 420$ nm with HWHM varied from 10 µm to 100 µm in 10 µm increments and from 100 µm to 200 µm in 50 µm increments, and on single subwavelength gratings (sw) with grating period $\Lambda_1 = 560$ nm ............73

Figure 35: Far-Field Diffraction Patterns: a) Far-field diffraction patterns for small numbers of grating lines in the first grating of a coupled pair with no gap between them. b) Far-field diffraction patterns for small numbers of grating lines in the first grating of a coupled pair with a 300 nm gap between them ........................................................................................................75

Figure 36: Far-field diffraction patterns for large numbers of grating lines in the first grating of a coupled pair with no gap between them ...................................75

xii
Figure 37: Perfect rotational alignment between fiber and borosilicate glass gratings. (b) 15-degree rotation of the fiber grating with respect to the borosilicate glass grating, giving rise to moiré fringes at an angle $\zeta$. 

Figure 38: Far-field output intensity map

Figure 39: Far-field pattern with fringe angle 16° resulting from the presence of a 5° fiber rotation

Figure 40: a) Line width variation in the second grating of a coupled pair, between 147 nm and 273 nm, interval representing a 30% variation on each side of the center line width, 210 nm. b) Far-field pattern for 30% line width variation. The pattern for a regular grating is also given for reference

Figure 41: a) Mirror symmetry positions around periodic defects. b) and c) Symmetric distribution of maximum intensities

Figure 42: a) Similar positions in periodically varied grating (period 13.86 µm). b) Maximum output intensities are the same for a first diffraction order at two similar positions (0 µm and 13.86 µm)

Figure 43: a) Stripped and cleaved fiber mounted in JEOL FIB machine. b) Fibers mounted in preparation for FIB

Figure 44: a) Top view of grating on facet of fiber #1. b) Cross-section of the grating

Figure 45: a) Gratings design in LayoutEditor. b) Varied grating design

Figure 46: EBL process flow on a glass substrate with an ESPACER charge dissipation agent and ZEP photo resist

Figure 47: SEM pictures of gratings fabricated on glass substrate. a) Top view of regular non-subwavelength grating. b) Cross section of regular non-subwavelength grating. c) Top view of regular subwavelength grating. d) Cross section of regular subwavelength grating. e) Top view of varied subwavelength grating

Figure 48: Complete test set-up for evanescent coupling

Figure 49: Green laser source

Figure 50: Checkered screen for fiber alignment with photodetector

Figure 51: With the 532 nm laser, the grating period on the fiber is non-subwavelength to the source. Therefore, higher diffraction orders were visible on the projection screen.
Figure 52: Actual test set up ...........................................................................................................99

Figure 53: Fiber tip touching grating on glass. The fiber forms a straight line with its mirror reflection, suggesting perpendicularity with glass surface...............100

Figure 54: Diffraction pattern of non-subwavelength grating; a) on opaque screen and b) as recorded by power meter .........................................................................................100

Figure 55: Observed pattern resulting from evanescent coupling .................................................101

Figure 56: Scanning results for a 560 nm – 480 nm SWG pair recorded by power meter, overlaying corresponding simulation results.................................................................102

Figure 57: The photodetector is placed at a diffraction angle to capture the higher order at its maximum intensity........................................................................................................103

Figure 58: Simulation schematic of the coupled SW gratings. a) Original simulation layout. b) Re-simulation layout from SEM analysis.................................................................104

Figure 59: Simulation output intensity results for 2D and 3D original simulation layout and re-simulation layout from SEM analysis.................................................................105

Figure 60: Simulation and experimental results for re-simulated CSWG pairs with different gap separations a) 560 nm – 420 nm pair b) 560 nm – 480 nm pair.........................................................................................................................106
CHAPTER I: Introduction

1.1 Overview of Diffraction, Subwavelength and Coupled Gratings

1.1.1 Diffraction Gratings

A diffraction grating is a set of periodic spaced elements or grooves, usually of the same size, separated by a distance comparable to the wavelength of light under study. A reflection grating is made on top of a reflective surface, whereas a transmission grating consists of a grating overlaying a transparent surface. An electromagnetic wave or light source incident on a grating will, upon diffraction, have its electric field amplitude, phase, or both, modified in a predictable fashion. When the light is monochromatic, it is diffracted into distinct diffraction orders.

In equation (1), \( \theta_i \) is the incidence angle with respect to the grating normal, \( \theta_d \) the angle of diffraction (negative for transmission and positive for reflection), \( n_1 \) is the index on the incident side, \( n_{1,2} \) the index on either the incidence or refraction side (depending on whether reflection or transmission is being studied), and \( D \) is the total geometrical path difference between light from adjacent grating elements. This equation is illustrated in Figure 1 for the transmission case.

\[
D = n_1 \Lambda \sin \theta_i + n_{1,2} \Lambda \sin \theta_d. \tag{1}
\]

The law of interference says that only when the path difference equals a multiple of the whole wavelength \( \lambda \) of the light, will the light from adjacent grating elements be in phase, thus causing constructive interference which is the grating equation illustrated in equation (2).

\[
m\lambda = \Lambda(n_1 \sin \theta_i + n_{1,2} \sin \theta_d) \tag{2}
\]
At all other angles $\theta_d$, are higher diffraction orders (or spectral orders), $m = 0, \pm 1, \pm 2, \ldots$, from the diffraction grating.

Figure 1: Total geometrical path difference between light from adjacent grooves in a transmission grating

1.1.2 Subwavelength Gratings

The period of subwavelength gratings (SWGs) is smaller than the wavelength of the incident light source. In this regime equation (2), called the grating equation, is true for only $m = 0$ which is always possible, and the propagating zeroth diffraction order still exists. Otherwise, only evanescent waves are present at the surface of the grating in the near field region. To identify what is considered the subwavelength condition for transmission, $m$ is assigned the value of 1 and equation (2) is transformed into an inequality to prevent having the first diffraction order. As a result, $\theta_d = 90^\circ$, $\sin \theta_d = 1$, and we have

$$\lambda > \Lambda(n_1 \sin \theta_i + n_2).$$

Adjusting the inequality, the subwavelength condition is represented as:
\[ \Lambda < \frac{\lambda}{n_1 \sin \theta_i + n_2}. \]  

(4)

The parameters of subwavelength gratings can be tailored for many applications, and SWGs have been used as polarizers [1, 2], high-reflectivity mirrors [3-5] and anti-reflection devices [6, 7]. They have also been applied towards biosensing [8], guided optics [9], optical couplers [10], apertureless microscopy [11, 12], nanoelectromechanical devices [13], and in nanoscale measurement [14].

1.1.3 Coupled Gratings

Figure 2: a): Plane wave source incident on coupled SWGs. Higher diffraction orders are exhibited at the output. b) Bonded pair of subwavelength gratings. c) Simulation of CSWGs. d) simulated far-field output intensity of the first diffraction order for different gaps between the gratings [15]
In [14], Rogers, et. al demonstrated the use of SWGs for measuring nanometer displacement of a MEMS accelerometer by coupling two subwavelength gratings wherein the second grating recoupled the non-propagating evanescent waves generated by the first grating into propagating light visible in the far field, as shown in Figure 2. The output intensity of the coupled light correlated to the distance between the two gratings.

1.2 Research Purpose

The picometer displacement resolution demonstrated in coupled SWGs [15] showed potential in investigating such structures for non-destructive bonding integrity evaluation. The value of this technology emerges from its facilitation of device testing, especially after fabrication and packaging.

This optical implementation circumvents the misalignment challenges that would necessitate bulky positioning equipment [16]. This is accomplished by the use of an optical fiber as delivery medium, as seen in Figure 3. A microlens could be fabricated directly on the input fiber facet to facilitate coupling with an external laser [17]. The first grating of the coupled pair is milled directly on the output fiber facet and once placed in the security system, the relative position of the coupled gratings is fixed. Any attempt to open, alter, or invade the device will result in the separation of the CSWGs, causing the EW coupling to be lost: this is the tamper evidence verification component of this proposed work. In Figure 3(a), tampering is evident by visibly observing far-field diffraction transmitted through a bottom optical window. If far field diffraction is present
the device is intact and has not been tampered with. This is due to the complexity of aligning and coupling SWGs with less than a 1 µm gap separation.

Figure 3: a) In-package implementation of CSWGs chip security system. b) On-chip implementation of the system

In another implementation, shown in Figure 3(b), the output of the coupled gratings is captured through a top optical window by reflection. As a result of the diffraction angle being much larger than the acceptance angle, the higher orders of diffraction do not re-enter the optical fiber. The layer of reflective material is located above the protected chip, also providing an additional barrier of protection against physical intrusion. Both
approaches allow nondestructive inspection without the need to open a sealed package and are integrated into the fabrication process.

![Graph showing far-field intensity (dB) vs angle (degrees) for varied CSWGs 1 and 2.]

Figure 4: Two instances of varied CSWGs generate two different signatures, while the first and second diffraction order are clearly visible.

Engineered defects can also be combined with the physics of CSWGs to create “fingerprints” for device chips, and allow verification of identity in addition to tamper evidence. In contrast to previously developed coupled gratings featuring fixed periods in each grating [14], a local random variation can be introduced in one of the gratings making up the system. This slight variation of one of the grating patterns in the pair of coupled gratings differentiates this specific set of gratings from another one, while the general output of each system remains essentially the same. This feature translates into variations in the intensity pattern of transmitted waves, distinguishing one device from another, as displayed in the simulations results in Figure 4. This complete solution
provides both tamper evidence and authentication, which places it forward from the currently used DNA taggant [18].

1.3 Dissertation Organization

A brief overview of transmission gratings, subwavelength gratings and evanescent wave generation followed by the research purpose is presented.

Chapter II provides a background on the step-index optical fiber component used in this project, as well as the context in integrated security research motivating this project.

In Chapter III, Finite Difference Time Domain (FDTD) simulations, fabrication methods and test procedure used in this research are presented.

Chapter IV discusses in detail the FDTD simulation results for the various types of subwavelength and coupled subwavelength gratings.

In Chapter V, SW grating fabrication is presented in detail.

Chapter VI concludes with the test setup and physical testing of the coupled subwavelength gratings. Also, this chapter presents a comparison of the simulated and measured results of the coupled subwavelength gratings, and outlines future work on this novel security technique.
CHAPTER II: Background and Motivation

In this section, the principles of waveguides and of optical fibers, which are a critical constituent of the proposed device, will be discussed. Additionally, the motivation for this research is stated and comprehensive background review of integrated security research is presented.

2.1 Background on Optical Fibers

2.1.1 Dielectric Waveguides

Simply stated, optical fibers are waveguides. The principle of dielectric waveguides can be explained referencing the slab waveguide, in Figure 5. The refractive index of the central region, or core, is greater than the cladding material, and is able to capture light. This difference in the indices of refraction of the core and cladding creates a condition called total internal reflection (TIR) explained below.

Figure 5: The slab waveguide, two-dimensional waveguide. The y-dimension extends to infinity
When a wave is incident at an angle $\theta_1$ on the dielectric boundary from the higher index side, the refracted ray in the low index medium leaves at an angle $\theta_2$, related to the incident angle by:

$$\theta_2 = \sin^{-1}\left(\frac{n_{\text{core}}}{n_{\text{cladding}}}\sin \theta_1\right).$$

(5)

If $\theta_1$ is smaller than a critical angle given by

$$\sin \theta_c = \frac{n_{\text{cladding}}}{n_{\text{core}}}$$

(6)

we have the situation illustrated in Figure 6:

![Figure 6: Case of light transmitted from a denser to a less dense medium, when $\theta_1 < \theta_c$. The refracted ray in the low index medium leaves at an angle $\theta_2$](image)

However, if $\theta_1$ exceeds the critical angle, $\sin \theta_2$ will be greater than 1, and $\theta_2$ will be imaginary. The ray will not refract at the interface and the light will be trapped within the high index medium as illustrated in Figure 7.
Figure 7: In a waveguide, light is launched so that $\theta_1$ exceeds the critical angle, and total internal reflection imprisons the ray inside the core.

In order to satisfy the boundary condition, there will still be evanescent waves in the cladding, propagating close to the core, parallel to the waveguide, and decaying exponentially in the direction orthogonal to the boundary as shown in Figure 8.

Figure 8: The evanescent wave travels along the separating surface, parallel to the waveguide.
When the electromagnetic wave is passing through a waveguide, the electric and magnetic fields present a quantity of modes, or permitted patterns, determined by the dimensions and the indices of refraction of the waveguide. The modes will be discussed further using the electromagnetic wave theory. Maxwell's equations [19] give a mathematical explanation of the propagation of electromagnetic waves, or light. In differential form, these equations can be expressed as follows when we are considering a source-free, linear and isotropic medium [20]:

\[
\nabla \times \vec{E} = \frac{-\partial \vec{B}}{\partial t}, \tag{7}
\]

\[
\nabla \times \vec{H} = \frac{-\partial \vec{D}}{\partial t}, \tag{8}
\]

\[
\nabla \cdot \vec{B} = 0, \tag{9}
\]

\[
\nabla \cdot \vec{D} = 0. \tag{10}
\]

\(\vec{E}\) (V/m) and \(\vec{H}\) (A/m) are the electric and magnetic fields amplitudes; \(\vec{D}\) (C/m²) is the electric displacement vector or electric flux and \(\vec{B}\) (T) is the magnetic flux or magnetic induction, defined as

\[
\vec{D} = \varepsilon \vec{E}, \tag{11}
\]

\[
\vec{B} = \mu \vec{H}. \tag{12}
\]

where \(\mu = \mu_0 \mu_r\) and \(\varepsilon = \varepsilon_0 \varepsilon_r\), \(\varepsilon_0\) is the electric permittivity of free space (8.8541 x 10⁻¹² F/m²), \(\varepsilon_r\) is the relative electric permittivity or dielectric constant of the material, \(\mu_0\) is the magnetic permeability of vacuum (4\(\pi\) x 10⁻⁷ H/m²) and \(\mu_r\) is the magnetic permeability of
the material. We will limit ourselves to substances that are neither absorbing nor amplifying so that $\varepsilon$ is real.

By manipulation of equations (7) to (10), the simplification of this system in terms of the electric field amplitude is:

$$\nabla^2 \vec{E} - \mu \varepsilon \frac{\partial^2 \vec{E}}{\partial t^2} = 0. \quad (13)$$

Equation (13) is called the “wave equation”. It can also be obtained in terms of the magnetic field amplitude:

$$\nabla^2 \vec{H} - \mu \varepsilon \frac{\partial^2 \vec{H}}{\partial t^2} = 0. \quad (14)$$

In a Cartesian coordinate system, we can separate equations (13) and (14) into three components, and solve for each of them. A valid solution of (13) will be:

$$E_i(r, t) = E_{0i} \exp(j \vec{k} \cdot \vec{r}) \exp(-j\omega t) + \text{const} \quad (15)$$

where $i$ represents the $i$th component, $\vec{r}$ (units of $|\vec{r}|$: meters) the position vector, $\omega$ (units: radians/second) the angular frequency of the wave, and $\vec{k}$ (units of $|\vec{k}|$: radians/meter) the wavevector, pointing in the direction of propagation of the wave. The magnitude of the wavevector is the amount of phase adding up as the wave passes through a unit distance and is expressed as

$$k = |\vec{k}| = \frac{2\pi n}{\lambda} = \frac{\omega^2 \varepsilon \mu}{\lambda}. \quad (16)$$

$$n = \sqrt{\mu, \varepsilon} \quad (17)$$

is the index of refraction (unitless) of the medium and $\lambda$ (units: meters) is the wavelength. For nonmagnetic materials, $\mu_r = 1$, so (16) and (17) become
\[ k = \omega^2 \varepsilon \mu, \quad (18) \]

\[ n = \sqrt{\varepsilon_r}. \quad (19) \]

Equations (7) to (10) are applicable for regions of continuous physical properties. However, in the waveguide case, different materials are present, and when the properties of the material change suddenly, \( \vec{E}, \vec{H}, \vec{B}, \text{and} \ \vec{D} \) must comply with a certain number of boundary conditions, that we will specify below. The instance where the interface is planar is illustrated in Figure 9. Indices 1 and 2 indicate parameters related to medium 1 and 2 respectively, where \( \vec{n} \) is the normal to the interface.

The tangential components of the electric and magnetic fields are continuous [20]:

\[ \vec{n} \times \vec{E}_1 = \vec{n} \times \vec{E}_2 \quad (20) \]

\[ \vec{n} \times \vec{H}_1 = \vec{n} \times \vec{H}_2. \quad (21) \]

---

Figure 9: Discontinuity in material properties. When the properties of the material changes suddenly, \( \vec{E}, \vec{H}, \vec{B}, \vec{D} \) must comply with a certain number of boundary conditions: continuity of the tangential components of the electric and magnetic fields, continuity of normal components of the electric and magnetic fluxes.
The normal components of the electric and magnetic fluxes are continuous:

\[ \vec{n} \cdot \vec{D}_1 = \vec{n} \cdot \vec{D}_2, \quad (22) \]
\[ \vec{n} \cdot \vec{B}_1 = \vec{n} \cdot \vec{B}_2. \quad (23) \]

With non-magnetic media, equation (23) simplifies to

\[ \vec{n} \cdot \vec{H}_1 = \vec{n} \cdot \vec{H}_2. \quad (24) \]

Electromagnetic waves being transverse, the electric field, dependently of its direction, can be decomposed into Transverse Electric (TE) or Transverse Magnetic (TM). The TE field has no component along the z-axis and is perpendicular to the plane of incidence containing the normal to the interface and the k vector. In the TM case, the electric field is parallel to the plane of incidence (Figure 10).

![Figure 10: The modes can be categorized in terms of Transverse Electric field (TE) and Transverse Magnetic field (TM). The TE field is perpendicular to the plane of incidence containing the normal to the interface and the k vector. In the TM case, the electric field is parallel to the plane of incidence.](image)
When describing the propagation of a wave, we need to consider two important parameters: $\beta$, the longitudinal wavevector or longitudinal propagation constant, which is the propagation coefficient along the direction of propagation of the electromagnetic wave, which we chose to be $z$, and $\kappa$, the transverse propagation constant. They are expressed as

$$\beta = k \cos \theta, \quad (25)$$

$$\kappa = k \sin \theta \quad (26)$$

where $k$ is the wavevector introduced earlier, and $\theta$, which can only take certain discrete values, is the incidence angle at the core-cladding surface. Each value of $\theta$ is associated to a mode. The relationship between the three wavevectors is shown in Figure 11.

![Figure 11: The geometric relation between $\beta$, $\kappa$ and $k$. $\beta$ is the propagation coefficient along the direction of propagation of the electromagnetic wave, which we chose to be $z$, and $\kappa$ is the transverse propagation constant.](image)

In order to find the allowed values of $\theta$, and the number of modes of the slab waveguide, we will consider a wave traveling inside the slab (Figure 12).
The light subjected to TIR is reflecting throughout the core of the fiber. At reflection points, the wave accumulates a different phase with respect to the incident ray, and there is interference. For the propagation to continue, this interference must be constructive, which implies that the phase difference between points A and C must be \( m \times 2\pi \), where \( m \) is a positive integer. If the phase change at reflection is \( \phi \), because of the two reflections at A and B we have \( 2\phi \) between the points A and C. So the waveguide condition for propagation will be:

\[
k (AB + BC) - 2\phi = m \times 2\pi \quad (27)
\]

or

\[
k (2d \cos \theta) - 2\phi = m \times 2\pi, \quad (28)
\]

and results in

\[
\frac{2\pi m \times d}{\lambda} \cos \theta_m - \phi_m = m\pi. \quad (29)
\]
For each \( m \), there is a \( \theta_m \) and a different interference pattern. Each of these field patterns is called a mode with the corresponding mode number \( m \). The smaller the angle \( \theta \), the higher the order of the mode will be. The order number indicates how many zeros the field has across the fiber for that mode.

The slab waveguide structure does not vary in the z-direction, and it is assumed that its length \( L \gg \lambda_0 \), which is the free space wavelength. The spatial index of refraction distribution comes to be

\[
 n (x, y, z) = n (x, y). \tag{30}
\]

In dielectric materials, \( n \) is real, so the optical energy cannot be absorbed, and a guided wave traveling along the \( z \)-axis retains all its energy. Therefore, the electric field for the guided wave that is a solution to Maxwell’s equations must have the form

\[
 \tilde{E} (x, y, z) = \tilde{\Omega} (x, y) \exp [j (\beta z - \omega t)] \tag{31}
\]

to ensure that the power circulation is along the \( z \)-direction exclusively. The magnetic field has the same \( \exp [j (\beta z - \omega t)] \) dependence. Separating the components changes the curls equations (7) and (8) to the forms:

\[
\begin{align*}
\frac{\partial E_y}{\partial y} - j \beta E_x &= j \omega \mu_0 H_x & (32a) \\
 j \beta E_x - \frac{\partial E_y}{\partial x} &= j \omega \mu_0 H_y & (32b) \\
 \frac{\partial E_x}{\partial x} - \frac{\partial E_y}{\partial y} &= j \omega \mu_0 H_z & (32c)
\end{align*}
\]

\[
\begin{align*}
\frac{\partial H_z}{\partial y} - j \beta H_y &= -j \omega \varepsilon E_x & (33a) \\
 j \beta H_x - \frac{\partial H_z}{\partial x} &= -j \omega \varepsilon E_y & (33b) \\
 \frac{\partial H_x}{\partial x} - \frac{\partial H_y}{\partial y} &= -j \omega \varepsilon E_z & (33c)
\end{align*}
\]

The slab waveguide in study presents no change along the \( y \)-direction, so \( \partial \tilde{E} / \partial y = 0 \) and \( \partial \tilde{H} / \partial y = 0 \). Equations (32) and (33) simplify to:
\[
\begin{align*}
-\beta E_y &= \omega \mu_0 H_x \quad (34a) \\
j \beta E_x - \frac{\partial E_y}{\partial x} &= j \omega \mu_0 H_y \quad (34b) \\
\frac{\partial E_y}{\partial x} &= j \omega \mu_0 H_z \quad (34c) \\
\beta H_y &= \omega \varepsilon E_x \quad (35a) \\
j \beta H_x - \frac{\partial H_y}{\partial x} &= -j \omega \varepsilon E_y \quad (35b) \\
\frac{\partial H_y}{\partial x} &= -j \omega \varepsilon E_z \quad (35c)
\end{align*}
\]

In TE modes we find only \(E_y\), \(H_x\) and \(H_z\) field components. From equations (34a) and (34c), \(H_x\) and \(H_z\) can be expressed as functions of \(E_y\):

\[
H_x = -\frac{\beta}{\mu_0 \omega} E_y, \quad (36)
\]

\[
H_z = -j \frac{1}{\mu_0 \omega} \frac{\partial E_y}{\partial x}. \quad (37)
\]

By replacing equations (36) and (37) in equation (14), we obtain a second order differential equation for \(E_y\):

\[
\frac{\partial^2 E_y}{\partial x^2} + \left(\mu_0 \omega^2 \varepsilon - \beta^2\right) E_y = \frac{\partial^2 E_y}{\partial x^2} + (k^2 - \beta^2) E_y
\]

\[
= \frac{\partial^2 E_y}{\partial x^2} + \kappa^2 E_y
\]

\[
= 0. \quad (38)
\]

A solution to the above equation must be found in each dielectric region to obtain the permitted modes. We will then make use of the boundary conditions to join these solutions. To be contained within the waveguide, the fields must produce standing waves inside the slab and evanescent waves outside. As a result, the following solutions are obtained:
for \( x > d/2 \):
\[
E_y(x) = A \exp(-\gamma x) \tag{39a}
\]

for \(-d/2 < x < d/2\):
\[
E_y(x) = B \cos(\kappa x) + C \sin(\kappa x) \tag{39b}
\]

for \( x < -d/2 \):
\[
E_y(x) = D \exp(\gamma x) \tag{39c}
\]

where \( A, B, C, D \) are constants to be calculated from the boundary conditions, and we designate \( \gamma \) as an attenuation coefficient:
\[
\gamma = \sqrt{\beta^2 - k^2}. \tag{40}
\]

Because of the symmetry of the index structure, the modes can be divided in two groups, symmetric (cosines) and antisymmetric (sines). In a symmetric mode, the amplitude is highest at \( x = 0 \), which is verified for \( C = 0 \). The symmetry also leads \( A = D \). We can then specify a symmetric mode as follows:

for \( x > d/2 \):
\[
E_y(x) = A \exp(-\gamma x) \tag{41a}
\]

for \(-d/2 < x < d/2\):
\[
E_y(x) = B \cos(\kappa x) \tag{41b}
\]

for \( x < -d/2 \):
\[
E_y(x) = A \exp(\gamma x). \tag{41c}
\]

For an antisymmetric mode, the amplitude is zero at \( x = 0 \) and the tails are of opposite signs. This is true when \( B = 0 \) and \( A = -D \). Thus we have:

for \( x > d/2 \):
\[
E_y(x) = A \exp(-\gamma x) \tag{42a}
\]

for \(-d/2 < x < d/2\):
\[
E_y(x) = C \sin(\kappa x) \tag{42b}
\]

for \( x < -d/2 \):
\[
E_y(x) = -A \exp(\gamma x). \tag{42c}
\]

The conditions that link the solutions at the boundaries are the continuity of the tangential components of \( \vec{E} \) and \( \vec{H} \) and their derivatives at \( x = -d/2 \) and \( x = d/2 \).

At \( x = d/2 \) and \( x = -d/2 \), the continuity requirement for \( E_y \) gives:

symmetric TE mode: 
\[
B \cos(\kappa \frac{d}{2}) = A \exp(-\gamma \frac{d}{2}) \tag{43}
\]
antisymmetric TE mode: \[ C \sin \left( \frac{\kappa d}{2} \right) = A \exp \left( -\frac{\gamma d}{2} \right) \] (44)

Writing B and C in terms of A, the field description becomes:

for \( x > d/2 \):
\[ E_y (x) = A \exp (-\gamma x) \] (45a)

for \(-d/2 < x < d/2\) :
\[ E_y (x) = A \frac{\exp \left( -\frac{\gamma d}{2} \right)}{\cos \left( \frac{\kappa d}{2} \right)} \cos (\kappa x) \] (symmetric TE mode) (45b)
\[ E_y (x) = A \frac{\exp \left( -\frac{\gamma d}{2} \right)}{\sin \left( \frac{\kappa d}{2} \right)} \sin (\kappa x) \] (antisymmetric TE mode) (45c)

for \( x < -d/2 \):
\[ E_y (x) = A \exp (\gamma x) \] (symmetric TE mode) (45d)
\[ E_y (x) = -A \exp (\gamma x) \] (antisymmetric TE mode). (45e)

From equation (38), we can see that \( \partial E_y/\partial x \) is made continuous at the boundary, the tangential magnetic field will also continuous as well:

symmetric TE mode: \[ \kappa B \sin \left( \frac{\kappa d}{2} \right) = \gamma A \exp \left( -\frac{\gamma d}{2} \right), \] (46a)

antisymmetric TE mode: \[ \kappa C \cos \left( \frac{\kappa d}{2} \right) = -\gamma A \exp \left( -\frac{\gamma d}{2} \right). \] (46b)

The equations satisfying the boundary conditions combine to give the eigenvalues equations:

\[ \tan \left( \frac{\kappa d}{2} \right) = \frac{\gamma}{\kappa} \] (symmetric TE mode), \[ \tan \left( \frac{\kappa d}{2} \right) = -\frac{\kappa}{\gamma} \] (antisymmetric TE mode). (47b)
The values of $\beta$ that satisfy these equations specify a discrete series of guided modes. The cross-section of the three first TE modes for the electric field of a channel waveguide centered at $(0, 0, z)$ is shown in Figure 13.

Figure 13: The TE electric field patterns of the first three modes. The values of $\beta$ that satisfy the eigenvalues equations specify a discrete series of guided modes, alternatively symmetric and antisymmetric [21]
For the analysis of the TE modes, we needed to use only the \( E_y, H_x \) and \( H_z \) field components. The TM modes are constituted by only the \( H_y, E_x \) and \( E_z \) field components. The \( H_y \) field is usually derived by plugging into equation (13) the expressions of the two other fields with respect to it, obtained from equations (35a) and (35c). The differential equation is solved using boundary conditions.

Another parameter of interest of the slab waveguide is the effective index, defined as:

\[
\text{n}_{\text{eff}} = \frac{\beta}{k_0} = n_{\text{core}} \sin \theta
\]  

(48)

where \( k_0 = \frac{2\pi}{\lambda_0} \) is the magnitude of the wavevector in free space (\( n = 1 \)).

The effective index, which value is between that of the core and cladding indices (\( n_{\text{cladding}} < n_{\text{eff}} < n_{\text{core}} \)), can be referred to as an average index of the structure that determines the velocity of the propagation of the mode. It is the component of \( k \) in the direction of propagation. Its angle with the \( k \) vector gives the coupling angle.

2.1.2 Step-Index Optical Fibers

![Layers of a typical optical fiber: higher-index core, lower-index cladding and external coating](image)

Figure 14: Layers of a typical optical fiber: higher-index core, lower-index cladding and external coating
An optical fiber is composed in general of an inner glass core of higher index of refraction, embedded in a glass cladding of lower index. A polymer jacket, also called buffer coating, sheathes the structure. When the effective index is uniform across the core with an abrupt decrease at the core-cladding interface as shown in Figure 14, the fiber is referred to as a step-index optical fiber.

There exist two types of rays in a step-index fiber, meridional and skew rays. A meridional ray goes through the fiber axis between each reflection at the core/cladding interface and lies in plane containing the axis. A skew ray follows a helical path around the axis, without ever crossing it. Its projection on a plane perpendicular to the axis forms a regular polygon that can be closed or open, shown in Figure 15.

Due to its cylindrical shape, the exact solutions to Maxwell’s equations for the optical fiber are quite complicated [22]. To summarize, the meridional rays generate TE and TM modes analogous to the modes of the slab waveguide. Additionally, the skew rays give rise to hybrid modes called HE and EH depending on whether the E- or H-component is dominant respectively. As a result of the fiber being bound in two
dimensions as opposed to one in the case of the slab waveguide, two integers \( l \) and \( m \) are necessary to identify the modes.

Optical fibers used in communication have a very small index difference, and in this case the propagating waves are almost linearly polarized. Therefore the modes can be approximated by linearly polarized modes called LP modes, formed by the superposition of TE, TM, EH and HE modes. In a LP\(_{lm}\) mode, there are \( 2l \) maxima around a circumference and \( m \) maxima along a radius as can be seen in Figure 16.

![Intensity plot for the first six LP modes in an optical fiber](image)

Of the rays that are incident on an optical fiber, only the rays that will be subject to TIR once inside will propagate along that fiber. The propagating rays have to enter the fiber through an acceptance cone illustrated in Figure 17. Applying Snell’s law and considering the maximum angle of incidence:
\[ n_i \sin \theta_i = n_i \sin \left( \frac{\pi}{2} - \theta_c \right) \]

\[ = n_i \cos \theta_c \]

\[ = n_i \sqrt{1 - \sin^2 \theta_c} \]. \hspace{1cm} (49)

Figure 17: Acceptance cone of an optical fiber

Using equation (6),

\[ n_i \sin \theta_i = \sqrt{n_1^2 - n_2^2} = NA, \]

which is the definition of the numerical aperture of the fiber.

As important it is to have a basic understanding of the main components of the presented system in order to grasp its operation, it is also necessary to get a general view on the context of this research in order to appreciate the motivation behind it. Our device has for goal to offer a new and more effective technology for tamper evidence. Therefore, the next section presents a background on IC security research.
2.2 The Necessity for IC Security

The conception and manufacture of complex integrated circuits (ICs) and semiconductor devices entails a considerable amount of time as well as sophisticated engineering skills, which makes creating such devices an expensive activity. Additionally, ICs can contain software encoded in memories or they can be employed for purposes necessitating encryption in order to maintain the secrecy of valuable information. These ICs impact numerous sectors of the semiconductor industry, ranging from medical, to automotive, to aeronautics, to communications and to defense, which is why their tampering (interfering with them so as to misuse, alter or corrupt them [24]) and counterfeiting (their fraudulent imitation or forgery [25]) represent a serious problem [26]. The global investment on semiconductor research and development (R&D) increased by 7% from $48.7 billion in 2011 to $53.0 billion in 2012 [27]. Therefore, one can foresee an increase in tampering and counterfeiting activities resulting from insufficient security for the related intellectual property.

Indeed, IHS (formerly Information Handling Services), a market research firm, revealed in an April 2012 publication that the five most commonly counterfeited types of semiconductors represent $169 billion in potential annual risk for the international electronics industry [28]. The International Chamber of Commerce (ICC) stated that fake and pirated manufactured goods will reach a total value of up to $1,770 billion in 2015 [29]. With technology and data positioned in combat zones, and original critical military hardware replaced by counterfeits, the danger to security and safety is as a major concern by the United States Senate Armed Services Committee [30]. Another wake-up call was the capture in December 2011 of the US RQ-170 Sentinel surveillance drone fallen in
Iran, with the Iranian government claiming to have extracted secret information from the aircraft [31]. Aviation in general and medical devices both are high-risk targets because of the potential threat to human life. The seriousness of the situation is illustrated by the graph in Figure 18, which shows that there were four times more reported incidents where counterfeits were confirmed in 2011 than two years before, and this number is further increasing [32].

The challenges posed by counterfeits are twofold. The first challenge is how to protect an IC chip against piracy (unauthorized copy), so that neither its physical structure, logical operation, nor informational content can be discovered and replicated by a non-authorized entity. The second challenge is to verify chip integrity versus replicas. Many surveys have been written on the subject of IC security. An early
prominent publication, [33] provides with a taxonomy of attackers, gives examples of non-invasive and physical attacks, and goes over governmental and commercial protection techniques available at the time and their weaknesses. Later, [34, 35] add a brief description of the security levels as defined by IBM (International Business Machine) and FIPS (Federal Information Processing Standard)e, place attacks in non-invasive, invasive and semi-invasive categories and also describe several defense technologies against these types of attacks. Subsequently, [36] presents anti-counterfeiting approaches and initiatives, discusses general research challenges in that field, and describes several anti-counterfeiting methods. More recently [37, 38] give threat models, state-of-the-art defenses and the defenses metrics for different types of attacks, while [39, 40] classify components and counterfeit types, expose supply chain vulnerabilities, identify avoidance and detection measures and review the associated challenges.

This review investigates answers to the two challenges mentioned earlier: protecting chips against piracy and verifying their integrity. This review identifies different types of piracy methods used against ICs, the information obtained through tampering, and different classifications of security techniques. However, a different classification is introduced, in which the location of the protection measure, on the chip itself or in the package, is taken in consideration. On-chip security techniques are generally applicable only to new chips because of modifications in the design or fabrication steps. On the other hand, package-level solutions are independent from the device and can be added to old as well as new chips. In each category, the security goal (anti-tamper or authentication) adds further subdivision. Additionally, this chapter presents security
techniques that have been proposed, following the new classification, and a summary of the research in IC security is given. This chapter is concluded with the current active areas of research in IC security and their respective challenges are highlighted, and amongst them a new and novel solution that addresses the requirements for popular emerging system-on-chip technologies.

2.2.1 Types of Attacks

There are multiple approaches for counterfeiting a chip or accessing its sensitive data. As previously mentioned [40], counterfeit integrated circuits can be old ICs that are recycled, or new ICs that are overproduced, given false specifications or sold although defective; a counterfeit can also be a clone (copy).

When layouts or masks are not readily available for duplication purposes, or when critical information is located inside the device, some kind of probing becomes necessary. Historically those means have often involved damage to at least part of the chip; hence, they are commonly termed “attacks.” The types of attacks aimed at discovering the workings of a device or accessing information are classified as invasive, noninvasive, or semi-invasive by Skorobogatov and Anderson [41].

In an invasive attack, the packaging is removed in order to get immediate access to internal components. The IC can then be studied either by microprobing or reverse engineering. Microprobing involves placing a chip under a long-working-distance optical microscope, whereas test signals are received and monitored by a computer. Using a laser, the passivation layer (the inert layer preventing corrosion) is ablated or removed,
which allows probe access to the internal signal lines [33, 35]. A focused ion beam (FIB) can be used to etch/mill through multiple layers to access conductive lines. After locating the conductive line, the FIB deposits a metal, such as platinum, to connect the signal to the surface, making it more easily accessible to larger probes [42].

In reverse engineering, the different layers of an IC are imaged using a high resolution reflected-light microscope with camera to create a three-dimensional map of the structure. As a result of this destructive invasion method, the IC is often rendered unusable. However, if layers of an IC can be taken off without notably altering trapped charges, the stored information or software contained in the IC can be revealed, and reproduced or modified [33, 43].

With the continuing shrinkage of IC components, invasive attacks are becoming more difficult, extremely time-consuming, and require sophisticated instruments and skills. Conversely, noninvasive attacks constitute a lower-cost option for the attacker, as minimal equipment is required for that type of tampering. A noninvasive attack is the study of the IC by indirect means, also called side channels. This method generally consists of tapping the device wires for signal or radiations as illustrated in Figure 19, or connecting the IC to an external test circuit. Analysis of the signals coming through side-channels has been successfully demonstrated to obtain secret keys from secure devices easier, faster, and at lower cost than destructive attacks. Noninvasive observations can reveal the logical functions of circuit modules [34] and obtain stored information that is crucial for circuit functionality [44]. Additionally, there are no signs of tampering, illustrating the danger associated with this type of attack. Common noninvasive methods include:
Side-channel attacks use information leaked during system operation. The input, the output and the side channel information are combined to recover the secret information or key. Side-channel information can be included in the power consumption, timing, or electromagnetic emission of the device during the processing of secret information.

(1) Collecting timing information from operations associated with security: the time consumed by every input-output pair is recorded, whether it is a single operation or an entire function [45, 46].

(2) Looking at current or power consumption during changes of states. Amongst these methods, differential power analysis (DPA), extracts secret information from an integrated circuit as this IC performs the same predictable operations, by applying statistical correlation and error correction methods to data-dependent power traces collected at the supply pins [47, 48].

(3) Exploiting electromagnetic radiations that leak information on different components of a device. For one component these emanations are of various types, depend on the operation being performed by the device, and are a result of the characteristics of the component combined with its coupling with other neighboring components. With sensors judiciously chosen and positioned, it is possible to obtain
multiple views of operations [49]. This multidimensionality makes electromagnetic side channels even more effective than power analysis, which is only cumulative [50].

A semi-invasive attack is between noninvasive and invasive attacks. It can provide an enormous amount of information on a circuit without the cost or the time required by a full invasive attack. It is invasive to the device packaging only, with no damage to the passivation layer. Physical contact is not made with the internal lines and the IC remains functional. For instance, exposure to ultraviolet light rendered security fuses on early erasable memory and microcontrollers inoperative [34]. Other examples of semi-invasive methods have used infrared light to provide a view through the back surface of a chip [51], or thermal imaging to locate active areas [52], or a pico-second imaging circuit analysis (PICA) technique to detect optical emissions from the chip [53]. Other illustrations of semi-invasive methods are optical-beam-induced current (OBIC) [54] or light-induced voltage alteration (LIVA) [55]; both of them utilize laser scanning to detect the location and logic state of transistors. An outstanding semi-invasive attack is fault injection, in which atypical environmental conditions are instigated during cryptographic operation in order to uncover the internal states, and which can breach a circuit faster than noninvasive attacks [48, 56-58]. Fault injection employs power tampering, short clock signals, large temperature variations, external electromagnetic fields, and light attacks such as pulsed lasers or ultraviolet lamps [59-64] to alter the state of chosen transistors in the IC, allowing a pirate to figure out the operation of the IC and ways to bypass its security features.

Invasive, noninvasive and semi-invasive attacks are conducted on devices that have been already built. Another threat exists due to the worldwide distribution of IC
production currently, and the involvement of often untrusted contractors. This makes it possible for a malicious party to modify or insert stealth components in a circuit during any step of the supply chain. These rogue components will either disable the IC, cause it to behave differently or allow stealing information under specific conditions that will not happen during standard simulations and post-manufacturing tests. This type of attack is termed hardware Trojan [58, 65-73].

To summarize, the main features of the four types of attacks described above are compared in Table 1. Ideally, an anti-tampering device would not only be impervious to all four, but it would indicate if any attack were attempted against it. A desired feature that would allow a legitimate examiner to confidently ascertain that an IC is not a counterfeit would be continued improvement in device integrity. However, in a nonideal world, ideas for a completely tamper-proof and authenticatable IC are often well ahead of the technological means available to create such device, which is why security methods are classified according to the type of protection they offer.

<table>
<thead>
<tr>
<th></th>
<th>DEPACKAGING</th>
<th>PHYSICAL CONTACT WITH INTERNAL CIRCUITRY</th>
<th>FAST</th>
<th>EXPENSIVE</th>
<th>TAMPER-EVIDENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVASIVE</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SEMI-INVASIVE</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>NONINVASIVE</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HARDWARE TROJAN</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
2.2.2 Classification of IC Security Solutions

The number of patents filed on IC security is proof that it is a constant preoccupation. However, there are fewer IC security techniques released to the point of implementation in an experimental setting or for commercial or governmental purposes, and this is evidence of the complexity of the task at hand. With the various types and evolution of attacks, different classification approaches have been offered, in regards to the first challenge posed by counterfeits, i.e. tamper resistance.

One system simply follows the attack classification and considers which type of attack is being counteracted [41], based on the fact that most anti-tampering techniques offer a countermeasure against either invasive/semi-invasive or semi-invasive/noninvasive attacks; resistance against all three types of attacks usually comes from an integration of different solutions, each solution tackling one type of attack.

Large companies are highly targeted, and as a result put high-level solutions in place for protection. For example IBM, a leader in security systems, lists six security levels for electronic systems in general, according to the amount of expertise, time, and the equipment cost necessary to break these levels of defense [74]:

1. Level ZERO: no security features; no time, no cost;
2. Level LOW: little security; inexpensive and easy attack;
3. Level MODL: security against low-cost attacks; some expertise, cost up to $5,000;
4. Level MOD: moderate security; some expertise, time, cost up to $50,000;
5. Level MODH: advanced security; much expertise and time, cost over $200,000;
Level HIGH: security against all known attacks.
The US government, in the more specific framework of cryptographic modules for sensitive information, imposes the FIPS (Federal Information Processing Standard) 140-2 standard, established by the National Institute of Standards and Technology (NIST). This standard describes in increasing order four levels of security, as well as the active or passive nature of the protection [75], and any system performing cryptographic operations and used by the government or military must abide to it:

<table>
<thead>
<tr>
<th>SECURITY LEVEL</th>
<th>GENERAL REQUIREMENTS FOR ALL EMBODIMENTS</th>
<th>SINGLE-CHIP CRYPTOGRAPHIC MODULES</th>
<th>MULTIPLE-CHIP EMBEDDED CRYPTOGRAPHIC MODULES</th>
<th>MULTIPLE-CHIP STANDALONE CRYPTOGRAPHIC MODULES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Production-grade components (with standard passivation).</td>
<td>No additional requirements.</td>
<td>If applicable, production-grade enclosure or removable cover.</td>
<td>Production-grade enclosure.</td>
</tr>
<tr>
<td>2</td>
<td>Evidence of tampering (e.g., cover, enclosure, or seal).</td>
<td>Opaque tamper-evident coating on chip or enclosure.</td>
<td>Opaque tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.</td>
<td>Opaque enclosure with tamper-resistant seals or pick-resistant locks for doors or removable covers.</td>
</tr>
<tr>
<td>3</td>
<td>Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization response circuitry. Protected vents.</td>
<td>Hard opaque tamper-evident coating on chip or strong removal resistant and penetration resistant enclosure.</td>
<td>Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multichip Standalone Security Level 3 requirements.</td>
<td>Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/penetration attempts causing serious damage.</td>
</tr>
<tr>
<td>4</td>
<td>Environmental failure protection (EFP) or environmental failure testing (EFT) for temperature and voltage.</td>
<td>Hard opaque removal-resistant coating on chip.</td>
<td>Tamper detection envelope with tamper response and zeroization circuitry.</td>
<td>Tamper detection/response envelope with tamper response and zeroization circuitry.</td>
</tr>
</tbody>
</table>

Table 2: Recapitulation of the FIPS physical security requisites. ([75])
Level 1, the lowest level of security, requires typical passivation methods, for example a seal (protective) layer to counter environmental or other physical damage;

Level 2 enhances the physical security of Level 1 by making tamper evidence of the seal mandatory;

Level 3 intends to stop an unauthorized party from obtaining access to key security parameters stored inside the module, for example, by placing the module in a solid, opaque, hermetic enclosure to discourage access to the contents or ensuring that tampering will destroy the module;

Level 4 offers the highest level of security. It calls for active anti-tampering technologies or a combination of passive and active tamper-resistant layers. With active anti-tampering, a targeted IC will take some action when subjected to any suspicious activity. This event can be environmental conditions or variations outside of the normal working ranges of the module, such as voltage, photon detection, acceleration, strain, temperature, chemical reactions, or proximity. Typical reactions are erasure or destruction. Level 4 mechanisms are particularly helpful in physically unguarded settings.

Another system of classification is proposed in Figure 20. In a first division, it considers the location of the countermeasures. This organization stems from the fact that protection can be implemented in the device packaging or, more intimately, added to the chip. In order to integrate both challenges posed by counterfeits, authentication is included in addition to tamper resistance, and the security solutions are further partitioned according to which challenge they address. The following examination of IC security techniques uses this classification approach.
Figure 20: Security classification based on location and goal of the protection
2.2.3 IC Security Techniques

A. Chip-Level Security

A.1 Anti-Tamper

One of the first security issues tackled by IC manufacturers was attacks against erasable programmable read-only memories (EPROM). To prevent unauthorized access, they placed security fuses shielded by a metal cover opaque to ultraviolet light. The objective was to make the fuses hard to find and if found, difficult to manipulate by a pirate. In electrically erasable programmable read-only memories (EEPROM), inverted memory cells were made more resistant to UV light. Furthermore, to counter well-equipped and highly skilled entities that could resort to laser cutting or FIB machines to take away the protective metal, multiple fuses would be placed at different locations. This would affect the data contained in the memory and make it useless [35].

Some researchers have proposed changing the characteristics of the circuit elements. For example, FIB implants could reduce the switching speed of chosen logic gates, making the usual low speed test methods useless in establishing their correct logic functions [76, 77]. Also largely suggested has been camouflage. One example would make analog components look like digital components and hide the former amongst a digital IC [78]. Another illustration would be to configure false interconnection contacts in read-only memory (ROM) devices or in flash memory cells [79, 80]. In other instances, a lightly doped density (LDD) region called "channel block" would be placed between the active areas, where the dopant type of the channel block would determine if there is connection or not. However, the density would be so small that usual reverse engineering methods would not discover the presence or polarity of the implants [81-83].
These connections would not be made of metal wires, but instead they would be buried, making surface etch necessary [84-87]. Also, fake apparent metal connections and nonworking transistors looking like real ones would mislead a reverse engineer [88-94]. Another example uses fake features isolated by invisible etch stop films [95]. These methods do make reverse engineering harder by forcing the attacker into brute force, but at the cost of power, area and delay overheads [96].

Security fuses, FIB implants and camouflage seek mostly to protect against invasive attacks. On the other hand, various protection methods termed logic hardening have been proposed at the circuit level specifically against noninvasive and semi-invasive attacks.

A method against timing attack is to make all operations take the same amount of time [45, 68], but this is clearly at the cost of efficiency. Another technique with less negative impact on performance and also used against electromagnetic leakage is to blind, i.e. to modify the way a computation is conducted so that it is uncorrelated to timing or electromagnetic radiations [45]. Other timing countermeasures eliminate cache or modify the way data is cached [72, 73, 97, 98].

One way to counter DPA is to make power consumption constant. This can be achieved by using gates that consume power independently of their input values, i.e. dual-rail logic, where the logic is replicated using complement wires and gates [99-104]. An on-chip signal suppression circuit can be added without alterations to the encryption circuitry to prevent information escaping through the current supply pin side-channel to be acquired by differential power analysis. The total current drawn from the supply is maintained at a defined level. Since DPA receives information resulting from variations
in the supply current, when these variations are reduced, a pirate needs more power samples to differentiate information from noise. The number of necessary power traces can be made excessively large, rendering the attack very long and expensive for the attacker [105]. These countermeasures are accomplished at the price of higher power expenditure and larger circuit area.

Circuit-level solutions such as randomization or update of keys during computation are used as well against timing attacks, power analysis or electromagnetic leakage. Signal strength reduction can also be effective against both electromagnetic and power analysis attacks [106].

A great deal of research is also aimed at counteracting fault attacks. Input parameters are commonly protected using cyclic redundancy checks; processing parts by redundant computation, checks on algorithm-specific properties, or blinding of exponentiation algorithms; and program flow by a signature. In these cases the security requirements have to be balanced with hardware or time overhead. Inherent countermeasures, such as the choice of parameters, can also be used. These solutions are reviewed in more detail by [107-109].

Garbled circuits promise a general solution to all noninvasive and semi-invasive attacks, with circuit area comparable to existing countermeasures [110-115].

A.2 Authentication

The other challenge is authenticating a chip, in other words determining whether the chip is an original or not. For that the IC has to be marked by a key that is impossible or too costly to reproduce. Chip authentication data have traditionally been stored on
nonvolatile memory located on the chip itself. The basic measures to prevent unauthorized access to this information are encryption of the data and/or permanent disconnection of the fuses leading to the section of the memory where it is written. However, with the plurality of types of attacks available, those precautions are no deterrent to a skilled and determined pirate, thus prompting more sophisticated methods to encode the origin and identity markers of ICs.

One authentication method has been the adaptation of watermarking to hardware, which means embedding authentication information in the circuitry in a manner invisible to the user. Researchers at UCLA utilized unused portions of FPGA blocks to mark their circuits [116]. The circuit was divided in tiles, each tile having several possible instances. Two instances of the same tile had the same functionality and were interchangeable, but with different layouts with marking differently located as illustrated in Figure 21. One circuit instance was thus made up of a set of instances of diverse tiles. In this fingerprinting technique, although timing properties might vary from one tile instance to another, there was no effect on global performance, timing, or power consumption. However, the technique cannot be employed for application specific designs (ASICs), which use a single mask. A method suitable for ASICs was the assignment of a unique ID to each chip by appending a small section to the control path that could be programmed after manufacture [117]. Besides incorporating the unique ID into the functionality of the IC, this technique was the first that would allow assessment of the number of counterfeits in the event that piracy would be discovered. However, new solutions were needed that would not be limited to meter counterfeits, but would instead prevent their creation and
circulation. Methods allying anti-tamper with authentication at the chip level are reviewed next.

Figure 21: Example of the use of tiling for fingerprinting, with the Boolean function Out = (A ∩ B) ∩ (CUD). Since the function as well as the tile interface with adjacent design components are unchanging, the configurations shown are transposable.

A.3 Anti-Tamper with Authentication

An innovative method to assign a unique ID to each IC was the Integrated Circuit Identification Device (ICID), illustrated in Figure 22. That technique did not require any unusual processing steps, nor was post-manufacture encoding necessary. Identical transistors, forming an array, drove each a resistive load. Fabrication variations caused the current passing through this load to be random, and the corresponding voltage was converted to a bit string [118].

ICID was the first example of a Physically Unclonable Function (PUF), before the name was coined. This authentication method has been gaining in popularity for the past decade and takes advantage of unique characteristics that are inherent to each IC. Two identically functional instances of the same chip will have distinctive features that are due
to uncontrollable random imperfections created during fabrication [119]. This unique pattern is the key that identifies the chip, and cannot be duplicated. The key unlocks a secret set of challenge (applied physical stimulus) and response (unpredictable but repeatable device reaction), coming from an exponentially large pool of possibilities, for authentication. In addition, any probing attempt alters the PUF’s behavior, ruining the PUF and providing tamper evidence of invasive attack.

Other examples of integrated circuit-based PUFs are silicon PUFs. The first PUFs of this type, depicted in Figure 23, were arbiter-based PUFs where a latch determines which of two racing signals going through a sequence of MUX stages arrived first [119, 120]. Implemented for circuit authentication, they make use of delay information as parameters. To achieve reliability of those PUFs in environmental variations, relative
delay comparisons are taken into account [121]. Security is further enforced by the fact that the key is volatile and is only generated when the device is powered. However, arbiter-based PUFs display weakness in front of model-building and emulation attacks [122-124] and have low entropy, which limits their unpredictability [125]. Reliability problems, like the effects of aging, also need to be resolved.

![Figure 23: A basic parallel delay-based PUF is shown. The path segments are designed to have the same delay but manufacturing variations cause the delays to differ slightly. The rising edge goes through the two different paths and the one-bit output is determined by which path allows the rising edge to arrive faster.](image)

More reliability and simplicity were brought in a modification of the arbiter PUFs, applicable to both Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs) [126]. They use delay loops to generate Ring Oscillator Physical Unclonable Functions (ROPFs), simple circuits that oscillate with a frequency affected by fabrication variations and hence would not be predictable, but could still easily be established by a counter shown in Figure 24. ROPUFs have become one of the most widespread physical unclonable functions, seeking more security and smaller area [127-136], although the most recently proposed implementation [137] is not universal and its structure must be adapted to the type (analog, digital, or mixed) and size of the chip. Nonetheless, it seems that the security goal is still at a distance of being...
achieved, as a complete characterization of arbiter PUFs was demonstrated in [138] using backside photonic emission analysis, with the claim that this method is applicable to all delay-based PUFs.

Several publications treat of SRAM-based Physical Unclonable Functions [139-153]. This compact security method takes advantage of existing static random access memory cells (cells that hold data as long as power is supplied) that take consistently at power-up one of two arbitrary stable states, 0 and 1. One particular memory cell arrives at a state, always the same, determined by the manufacture process. A challenge is a subset of these memory cells; the response is their respective power-up state. Not all FPGAs offer uninitialized SRAM memory, and the idea is adapted with Butterfly Physical Unclonable Functions (BPUFs) that use cross-coupled latches, do not require any power-up for assessment, and are appropriate for all sorts of FPGAs [154]. However latch-based PUFs are less robust to temperature variations than SRAM PUFs [125].
In any case, settling-state-based PUFs such as SRAM and BPUFs lack the level of security expected from a PUF, as SRAM PUFs have been characterized by FIB circuit edit and laser stimulation, and cloned [155, 156].

More recent popular PUF developments at the chip level include the following:

(1) Glitch PUFs relying on delays, use glitches in combinatorial logic circuits [157-160].

(2) Secret Model PUFs associated with physical PUFs, mimic the PUF challenge-response activities, lessening the required amount of storage for challenge-response pairs [161-164].

(3) Public PUFs or PPUFs, defined as “multiple-input–multiple-output systems that are much faster to execute than they are to simulate, and whose security no longer relies on the secrecy of their physical parameters as PUFs do” [165], can be modeled, but the model evaluation requires much more work and time than the evaluation of the PUF itself [163, 165-169]. The same idea appears in SIMPL systems (Simulation Possible but Laborious systems) [170-173].

A concept completely different from PUFs, the Secure Split-Test (SST) [174] proposes to place two blocks, a functional-locking block to guarantee that only ICs unlocked by the intellectual property (IP) owner have correct functionality and a scan-locking block to ensure that functional results cannot be scanned out and subsequently allow tampering with the protection hardware. In addition to the area overhead created by the additional blocks, the multiple exchanges between the IP owner and the foundry will add to the SST cost.
In the particular case of recycled ICs, i.e. components that are defective or used originals sold as new and working out of specification, the natural course of action is to find a way to compare them to non-defective, unused chips. The absence of functional defect is ascertained through extensive testing. Once established that an IC is fully functional, the other parameter is its “length of service.” The circuit aging concept, first used for reliability assessment, has been recently applied to combat IC recovery by a research group in Connecticut. First, they proposed a comparison between two ring oscillators, the first a reference free of stress and the second a stressed ring aging rapidly [175]: the larger the difference between the rings frequency, the older the chip. The effects of temperature and inter-chip process variations are filtered out by data analysis. The two rings create minimal overhead and because they are bound to each other their relative frequency cannot be tampered with. Next, using instead the delay distribution of paths, the same researchers completely eliminate the area overhead [176, 177]. Indeed, the delay distribution being within a certain range, a larger delay indicates an older IC. This implementation is also applicable to legacy ICs and is completely tamper-proof, since it uses inherent properties of the circuit. However, with large process variations sufficient accuracy can be difficult to attain. A third embodiment uses counters to record usage time and an embedded antifuse memory block to store the recorded values [178]. The memory block cannot be reprogrammed, which makes it tamper-evident.

Another group compares the aging between similar parts of one circuit to create a signature [179], a method also applicable to legacy chips.

In the next subsection, we will consider package-specific security solutions.
B. Package-Level Security

B.1 Anti-Tamper

Protection has been often envisioned to be added as one or several supplementary layers, including extra circuitry for a response to tampering. For example, plates connected together and having serpentine or meandering conductor paths on them could be used as protective shielding against invasive or side-channel attacks [98, 180-182]. In other models, top and metal layers could be made more difficult and slower to etch than the passivation layer and the active circuitry [183], bonded substrates could support memory detectors on their external face [184], or an adhesive layer covered with porous material could send an electrical signal when torn [185]. Other examples would modify the packaging using a molding compound in which a change in capacitance or impedance would be detected by some circuitry [186, 187], add magnetic components to produce a magnetic response in elements situated on the target IC [188], or place reservoirs containing fluid chemicals that would destroy a circuit under reverse engineering attack [189, 190]. In another solution, a conductor is tightly wound around the protected IC and a detection circuit, all packaged together in a solid epoxy rendering the wires invisible from the outside; the winding of two devices is not exactly the same, even though they come from the same fabrication process [191]. However, this type of housing has the drawback of being complicated to build and consequently expensive to produce.

B.2 Authentication

Active research has been conducted for the past few years to tag ICs with biological deoxyribonucleic acid (DNA). According to its proponents, the DNA signature is
practically impossible to replicate, is inexpensive, requires only minimal change in the fabrication process, and is extremely accurate, the probability of a false positive authentication being one in a trillion [18]. It consists in an ink containing shuffled plant DNA to produce a quaternary sequence unique to each IC chip and kept in a database. This ink also fluoresces under certain light frequencies. The product derived from this research, SigNature® DNA, is marketed by Applied DNA Science and has been used on microchips by the Department of Defense [192, 193]. However, DNA is known for its sensitivity to harsh conditions [194], and the Semiconductor Industry Association (SIA) has shown reluctance to accept this technology as a general IC marking solution. The SIA does not believe SigNature DNA to be as reliable as presented, as it has not been independently evaluated or tested on a wide variety of products of different origins [195].

B.3 Anti-Tamper with Authentication

Other package security methods are armed with protection devices offering both tamper evidence and authentication capability.

The most widely known electromagnetic protection is probably the hologram [196], a type of diffractive optically variable image device (DOVID), often seen on smart cards. A hologram is a 3D picture showing different perspectives depending on its position with respect to the viewer, in an effect called parallax. Hidden and apparent authentication mechanisms can cohabit on a hologram. When positioned at the seal point of a package, a hologram also acts as a tamper-evidence device. However, available instruments are able to resolve conventional holograms in a matter of days [197, 198] and more sophisticated
added nanoscale features, for example those operating in the near-field regime [199] will probably be at the reach of state-of-the-art cloning apparatus as well.

PUFs, intrinsically tamper-resistant, are also used for authentication at the package level.

An optical PUF was suggested by Pappu, made of a transparent material, in which light scattering particles were inserted at random in the course of fabrication. When hit by a laser beam, the device would produce a speckle pattern, and minor variations in the location of just a few particles from one device to another would noticeably modify their whole interference patterns. In this implementation, the challenge set would be the position, angle amplitude and wavelength of the laser, and the response would be the speckle pattern [16]. Although fabrication of the light scattering token itself is a low-cost process, the depicted PUF involved pricey and sizeable equipment comprising a laser and a precise mechanical positioning system. The relative position of the laser, token and image sensor should be exactly the same every time the speckle pattern is recorded. Other authors [200]; [201-203] suggested an integrated version of the optical PUF where the incidence angle parameter would be replaced by the number of lasers that would be turned on or by switchable display pixels in a second embodiment. However in all cases, the smallest change in the token due to normal usage or environmental variations would change the speckle pattern and result in a false alert.

A magnetic PUF has been applied for card authentication, taking advantage of the noise-like permanent characteristics of magnetic stripes. The magnetic particles forming the stripes are of different sizes and shapes, randomly assembled, and emit an unchanging
and unique background signal [204-207]. Card readers must be adapted for the use of this magnetic PUF, which affects its cost.

Another type of PUF for package authentication might be created using an array of nanorods. During the development of an assembling method to form gold nanorods on a nanostructured surface, it was noted that although the same array pattern could be repeated, the individual nanorods varied slightly in length, orientation and separation with the previous nanorod in the array. This translated into a shift in color and intensity in their far-field imaging [208, 209]. Silver nanowires exhibit polarization-dependent surface-enhanced Raman scattering, that offers covert authentication because encrypted in the nanostructure [178].

Radio-Frequency Identification (RFID) labels [210] allow –as opposed to a conventional bar code –automatic identification of a tag from a distance with no line-of-sight necessary with the reader [211-213]. The tag is an antenna/microchip assembly and the reader is a second antenna emitting radio-frequency waves and receiving a response signal with information from the tag. However, by itself the tag is subject to easy cloning, which is why it is being associated with Coating Physical Unclonable Functions (COPUFs) or delay-based PUFs [210, 214-218] to form an “unclonable” tamper-evident RFID tag. COPUFs [219-221], which use a protection layer shielding an IC, are attractive because of their low manufacturing cost. The coating film contains dielectric particles that are random as to their dimensions, shape, and location. In Figure 25, metal line sensors arranged underneath the protective layer like a comb are employed to determine the local capacitance of the coating. These capacitances are random because of the random properties of the particles in the coating, and constitute the responses to voltage
challenges, each of different frequency and amplitude. Coating PUFs allow the detection of physical tampering, as a result of changes in the local responses, as well as device authentication. An insulating layer between the COPUF aluminum lines and the IC underneath acts as a barrier against crosstalk between sensors and protected circuit. However, these additional metal and insulation layers create a sizeable packaging overhead, and because the sensors have to be constantly active, power consumption is significantly increased.

Figure 25: Graphic cross-section of a Coating PUF IC. Aluminum sensors in the higher metal layer measure the local capacitance of the coating

When considering systems on a chip, which we will discuss in the next section, RFID allied to PUF does not present the best attributes for integrity solutions, because of the opacity of COPUFs [219] and reliability issues [121] associated with delay-based PUFs. As for holograms, available instruments are able to resolve conventional holograms in a matter of days [197, 198] and more sophisticated added nanoscale features, for example those operating in the near-field regime [199] will probably be at the reach of state-of-the-art cloning apparatus as well.
Table 3: Summary of Security Solutions

<table>
<thead>
<tr>
<th>SECURITY SOLUTION</th>
<th>PROTECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuses</td>
<td>Counter advanced invasive attacks such as laser cutting or FIB</td>
</tr>
<tr>
<td>Change of element characteristics</td>
<td>Makes usual invasive test methods useless</td>
</tr>
<tr>
<td>Logic hardening</td>
<td>Hardens circuit against noninvasive and semi-invasive attacks</td>
</tr>
<tr>
<td>Tiling</td>
<td>Authenticates without effect on performance, timing or power of FPGA</td>
</tr>
<tr>
<td>Post-manufacture programming</td>
<td>Allows metering when counterfeiting is discovered</td>
</tr>
<tr>
<td>Silicon PUFs</td>
<td>Authenticate thanks to a unique volatile pattern that cannot be duplicated (or take too long to simulate in the case of PPUF), are destroyed by physical tampering</td>
</tr>
<tr>
<td>Secure Split-Test (SST)</td>
<td>Guarantees that only ICs unlocked by IP owner have correct functionality and prevents tampering with the protection hardware</td>
</tr>
<tr>
<td>Aging</td>
<td>Allows identification of recovered ICs, is tamper evident</td>
</tr>
<tr>
<td>Shielding</td>
<td>Protects the IC with a tamper-proof enclosure</td>
</tr>
<tr>
<td>SigNature DNA</td>
<td>Offers unique sequences for authentication</td>
</tr>
<tr>
<td>Holograms</td>
<td>Offer covert or overt authentication, are tamper-evident when placed at seal point of package</td>
</tr>
<tr>
<td>Magnetic PUF</td>
<td>Offers a unique fingerprint for authentication, is tamper evident</td>
</tr>
<tr>
<td>Optical PUF</td>
<td>Offers a unique pattern for authentication with complex output and hard modeling, is tamper evident</td>
</tr>
<tr>
<td>Nanorod/nanowire arrays</td>
<td>Translate into a possibly covert, unique shift in color and intensity in their far-field imaging for authentication, are tamper evident</td>
</tr>
<tr>
<td>RFID + COPUF</td>
<td>Allows identification from a distance, no line-of-sight necessary, is tamper evident</td>
</tr>
</tbody>
</table>

2.2.4 Integrity Solutions for Systems On a Chip

For the past decade there has been an increased focus on 3D Heterogeneous Systems on a Chip (3D-HSoC) [222-235] and an explosion of wearable devices that carry a lot of personal information [236-248]. These chips are custom-produced in small quantities and hence carefully controlled. A usual way of inspecting them is to open the package, study individual chips and then repackage the device for reintegration into the supply chain. Nevertheless, with the security and privacy issues entailed with these systems, there has been a growing recognition of the need to bury passive covert tamper-evident solutions in packages to provide clues in the instance the initial technologies would be compromised. The prospect of generalized use of Systems on a Chip (SOCs) and wearable devices makes it useful to get a global view of the research directions applicable
to the security of these types of ICs. Table 3 provides a summary of the security solutions examined in this survey.

Figure 26: Schematic of the coupled subwavelength grating setup. Source: A.-A. Rogers, "Evanescent wave coupling using subwavelength gratings for optical MEMS accelerometer," PhD Dissertation, Electrical Engineering, University of South Florida, Tampa, FL, 2011

A mandatory attribute for SOCs and wearable devices is compactness. However, the most critical aspects of these chips being sensitive information protection and reliability, it is paramount to ally anti-tampering with device authentication. A single solution offering both security features would be preferable to respect the compactness requirement. Additionally, it would be very convenient if one did not need to access the IC itself to check if it has been tampered with or to authenticate it, the packaging giving all this information. With the stealth nature of the security desired, optical means come to mind. A few solutions using optical structures such as Fabry-Perot (FP) cavities or gratings promise the possibility of detecting nanometer-range displacements induced in the casing by any physical intrusion attempt. However, these systems are usually bulky structures including servomechanism feedback loops, multiple mirrors, beam splitters, amplifiers or differential circuits [249-254]. With the stealth nature of the security
desired, newer optical means such as CSWGs, featuring a plain laser-gratings-photodetector setup, shown in Figure 26, are of choice.
CHAPTER III: Methodology

This research aims to use this CSWG method for tamper verification of electronic chips and also for device authentication. The envisioned device will be comprised of an encased optical system which transmits a laser source through an optical fiber that has SWGs etched into the output facet of the optical fiber, and into a glass substrate with SWGs of a different period etched into its surface. Computer simulations guide the design for optimal operation of the security solution. The optical setup is demonstrated using the optical modeling software, Optiwave™ OptiFDTD to validate the evanescent wave (EW) coupling concept reported in this dissertation with the following characteristic parameters: a Gaussian wave incident source with wavelength $\lambda = 0.65 \mu$m, a subwavelength (SW) grating in the output facet of a silica optical fiber, and a SW grating in a borosilicate glass substrate. The 3D design and 2D projection are shown in Figure 27.

The period and thickness of the gratings are optimized for maximum evanescent wave coupling efficiency, and the size of the input light beam and the number of grating lines is established for discernible transmission of higher diffraction orders at a wavelength of 650 nm. The gratings are fabricated on a silica fiber using focused ion beam milling and on a glass substrate using e-beam lithography. The measured output results are compared to simulation results.

This chapter exposes the mathematics behind our simulation software, and the rationale for our parameters, instrumentation and fabrication methods choices.
3.1 Optical Simulations with Finite Difference Time Domain (FDTD)

We designed coupled regular and varied gratings, with several line width distributions for the varied gratings using OptiFDTD, a photonics simulation software by OptiWave [239].

The Finite Difference Time Domain (FDTD) method was initially presented by Kane S. Yee, in 1966 [255], and is today amongst the most widespread techniques applied to model electromagnetic problems. Yee suggested the approximation of Maxwell's curl equations, repeated here:
\[ \nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t} \quad (51) \]
\[ \nabla \times \vec{H} = \frac{\partial \vec{D}}{\partial t} \quad (52) \]

with three-dimensional central differences. Since the medium is assumed linear, the following constitutive relations are true:

\[ \vec{D} = \varepsilon \vec{E} \quad (53) \]
\[ \vec{B} = \mu \vec{H} \quad (54) \]

Using the differential form, we can thus express (51) and (52) as:

\[
\begin{align*}
\frac{\partial E_x}{\partial t} &= \frac{1}{\varepsilon} \left( \frac{\partial H_y}{\partial y} - \frac{\partial H_z}{\partial z} \right) \quad (55a) \\
\frac{\partial E_y}{\partial t} &= \frac{1}{\varepsilon} \left( \frac{\partial H_z}{\partial z} - \frac{\partial H_x}{\partial x} \right) \quad (55b) \\
\frac{\partial E_z}{\partial t} &= \frac{1}{\varepsilon} \left( \frac{\partial H_x}{\partial x} - \frac{\partial H_y}{\partial y} \right) \quad (55c)
\end{align*}
\]

\[
\begin{align*}
\frac{\partial H_x}{\partial t} &= -\frac{1}{\mu} \left( \frac{\partial E_y}{\partial y} - \frac{\partial E_z}{\partial z} \right) \quad (56a) \\
\frac{\partial H_y}{\partial t} &= -\frac{1}{\mu} \left( \frac{\partial E_z}{\partial z} - \frac{\partial E_x}{\partial x} \right) \quad (56b) \\
\frac{\partial H_z}{\partial t} &= -\frac{1}{\mu} \left( \frac{\partial E_x}{\partial x} - \frac{\partial E_y}{\partial y} \right) \quad (56c)
\end{align*}
\]

To be able to use FDTD, a computational domain, or space where the calculation will be carried out, must be chosen. The E and H fields will be established at every point pertaining to the computational domain. Each material lying inside the computational domain must be indicated, using the index of refraction. The simulation region must be partitioned into "Yee Cells" in order for the FDTD method to be employed. The six field components in each Yee cell, E_x, E_y, E_z, H_x, H_y and H_z, are separated to each other by half a space step as shown in Figure 28.
The time increment and the spatial discretization are bound; we can notice from (55) and (56) that the time derivative of the E-field is determined by the curl or variation across space of the H-field, and vice-versa. These equations are transformed into central-difference equations and discretized to allow the numeric calculations. To facilitate computer implementation, they are arranged so that the indexes are integers. We then have:

\[
\begin{align*}
E_{x(i,j,k)}^{n+1} &= E_{x(i,j,k)}^n + \frac{\Delta t}{\varepsilon} \left( \frac{H_{z(i,j,k)}^{n+\frac{1}{2}} - H_{z(i,j,k-1)}^{n+\frac{1}{2}}}{\Delta y} - \frac{H_{y(i,j,k)}^{n+\frac{1}{2}} - H_{y(i,j,k-1)}^{n+\frac{1}{2}}}{\Delta z} \right) \\
E_{y(i,j,k)}^{n+1} &= E_{y(i,j,k)}^n + \frac{\Delta t}{\varepsilon} \left( \frac{H_{z(i,j,k)}^{n+\frac{1}{2}} - H_{z(i,j,k-1)}^{n+\frac{1}{2}}}{\Delta z} - \frac{H_{x(i,j,k)}^{n+\frac{1}{2}} - H_{x(i,j,k-1)}^{n+\frac{1}{2}}}{\Delta x} \right) \\
E_{z(i,j,k)}^{n+1} &= E_{z(i,j,k)}^n + \frac{\Delta t}{\varepsilon} \left( \frac{H_{y(i,j,k)}^{n+\frac{1}{2}} - H_{y(i,j,k-1)}^{n+\frac{1}{2}}}{\Delta y} - \frac{H_{x(i,j,k)}^{n+\frac{1}{2}} - H_{x(i,j,k-1)}^{n+\frac{1}{2}}}{\Delta x} \right)
\end{align*}
\]
In the equations, the E and H fields are separated in time by \( \frac{1}{2} \Delta t \) intervals. The new H field components are calculated at \( n + \frac{1}{2} \) from the previous field components by means of (54a) to (54c). Then the new E field components at \( n + 1 \) are determined using (53a) to (53c). The process is then reiterated as many times as necessary in a leapfrog manner, until the final time step is attained.

The speed of light restricts the transmission of information during a time \( \Delta t \) to a distance \( c \Delta t \). To avoid an unlimited increase of the calculated E and H components and ensure the stability of the model, the so-called Courant-Friedrichs-Lewy (CFL) Stability Criterion must be met [256]. This condition is given by:

\[
c \Delta t < \frac{1}{\sqrt{\frac{1}{\Delta x^2} + \frac{1}{\Delta y^2} + \frac{1}{\Delta z^2}}}, \quad c = \frac{1}{\sqrt{\mu \varepsilon}}
\]

so that we can incorporate in the numerical approach far-away points that can impinge on the time propagation. When this requirement is fulfilled, the grid is said to be “causally connected.”

After the computational domain and the materials that it contains have been specified, a source is identified. Given that the E and H fields are calculated directly, the result of the
simulation is generally the E or H field at a point or a succession of points within the computational domain.

FDTD allows for arbitrary model geometries and places no restriction on the material properties of the devices. It permits the precise characterization of complex inhomogeneous, lossy or even anisotropic material structures. As a direct solution of Maxwell's time-domain equations, the method is a comprehensive full-wave solution without approximations that would preclude an exact solution from being obtained. FDTD permits to determine the fields both inside and outside a structure. In particular, OptiFDTD allows easy generation of grating arrays using VBScript.

A disadvantage of FDTD is the fact that it demands the entire computational domain to be gridded, and these grids must be small compared to the smallest wavelength and smaller than the smallest feature in the model. When very large computational domains must be used, the consequence is extremely time-consuming simulations, and this makes arduous the modeling of long, thin features. The approach is memory demanding and lengthy for the reason that for each spatial grid point at each time step, it collects values and performs calculations. The translation of derivatives into finite differences causes the wave to progress slower than its real velocity of propagation. Our approach to overcome these limitations is to convert 3-D structures to equivalent two-dimensional models, less demanding in memory and time. This is achieved by calculations from the effective indexes. Similar schemes have been used before [257-261].

Finally, since the computational domain must be finite, a boundary condition must be stated. The boundary must be at a sufficient distance from the waveguide in order not
to diminish the exactness of the solution. The absorbing boundary condition replicates the effect of a highly lossy material outside the boundary.

3.2 Wavelength and Components Choice

A Gaussian wave of wavelength 0.65 \( \mu \text{m} \), normally incident on the gratings, was chosen as the illuminating light source, as opposed to a longer, non-visible infrared wavelength to permit visual inspection. The light was TE-polarized (i.e. the electric field is parallel to the gratings).

In a physical environment, it can be a challenge to perfectly align the light source to first grating #1 and grating #1 to grating #2. When the first grating is written directly on the fiber facet, the fabrication process eliminates misalignment of the beam, since the grating remains at a fixed position relative to the incident beam. The first grating was patterned on a silica fiber and the second SW grating in a borosilicate glass wafer, both substrates transparent at visible wavelengths.

3.3 Fabrication Methods

3.3.1 Electron Beam Lithography (EBL)

Electron-beam lithography (EBL) is a versatile method that can be used on diverse materials to create countless kinds of patterns. The substrate is covered with a film called a resist [262], sensitive to electrons. When a focused beam of electrons scans the resist following the desired pattern, the solubility of the exposed regions is changed. The resist is then immersed in a developer that will remove either the exposed or the non-exposed
regions, depending on the positive or negative nature of the resist. The technique steps for a typical resist patterning process are illustrated in Figure 29. Subsequent etching transfers the shapes drawn in the resist into the substrate.

![Figure 29: Steps of resist patterning in typical EBL process](image)

EBL can create structures with resolution below 10 nm. Although aberration and space charge play a large role in limiting resolution, other phenomena such as forward and backward scattering as well as generation of secondary electrons also contribute. Forward scattering is caused by elastic collision of the electrons entering the resist, which diverts the electrons and broadens the beam. Thicker resist results in more beam broadening, particularly at low incident energies [263]. Backward scattering is caused by neighboring features, leaking electrons into the new features, causing the proximity effect [264-266] broadening the image, and reducing contrast. Secondary electrons [267, 268] are produced by inelastic collisions of the incident electrons [269]. They have low energy and thus only nanoscale range but eventually limit the pitch resolution [270]. The use of higher energy electrons or thinner resist can reduce forward scattering, but there is no
way to prevent secondary electrons. The main disadvantage of this type of lithography is its slow speed.

3.3.2 Focused Ion Beam (FIB) milling

When a sample is three-dimensional or structures are already present, the use of a resist coating is not practical. The easiest method to create patterns in such cases is to mill them directly on the substrate using a focused ion beam (FIB). FIB milling consists in having the heavy ions such as Ga+ and Au+ in the incident beam elastically collide with atoms on the sample, thus dislodging them from the substrate [271]. The escaped atoms are either re-deposited or pumped out of the vacuum chamber. As with EBL, inelastic collisions create photons and secondary electrons.

Since it only takes a single step, FIB is much faster than EBL and can as well create structures down to the nanometer scale on a large variety of materials. It has been used to fabricate lenses on fiber tips [272], microlens arrays [273], pillar microcavities [274], stacked Josephson junctions [275], and photonic structures in diamond membranes [276, 277]. However, large doses of ions are necessary, which limits the area that can be patterned.

3.3.3 Charging

Due to electrons and ions being charged particles, they will likely charge a dielectric substrate because they are not able to rapidly find a path to ground. Negative charging repels the electron beam from the charged region whereas positive charging
attracts the electron beam to the charged region. Both produce substantial distortion during patterning [278]. A thin conductive film over or underneath the resist, for example a ten-nanometer thick layer of gold, gold-palladium, chrome, or aluminum, or a conductive polymer like TQV (Nitto Chemical Industry) or ESPACER100 (polyisothianaphthenesulfonate, Showa Denko) [279, 280], will solve this issue, providing a path to the resist with minimum scatter. The conductive coating is removed before development. ESPACER100 can be rinsed off with water and thus can be applied directly on numerous resists.

3.4 Test Procedure

Our approach to testing the coupled gratings system uses simulations related in Chapter IV, where the gratings dimensions and relative position are optimized and variations are introduced into one of the gratings.

The foundation of the coupled gratings testing requires correlation of the output intensity from the simulation results, with the measured output intensity. A test setup has been configured, where the fiber and glass substrate gratings are brought in contact using a nanomanipulator. The input is introduced using a laser and the output is collected by a photodetector. The assembly components will be discussed in more detail later in Chapter VI. Additionally, the testing results of the coupled subwavelength gratings are presented. The testing and simulation results will be compared, where the overall total system assessment will be described in detail.
CHAPTER IV: Simulation Results

The effects of beam size, number of lines, rotational misalignment on coupled subwavelength gratings (CSWGs), and of variations in the second grating of the coupled pair are investigated in this chapter using optical modeling. Although the effects of input beam size and finite number of grating lines has been studied for subwavelength gratings [281-285], to the best of our knowledge the influence on CSWGs has not been analyzed yet. Therefore, using finite difference time domain (FDTD) simulations [255], optimization of the gratings periods from both SW gratings, and observation of the effect the beam diameter, the number of grating lines written on the optical fiber facet, and the rotational misalignment between the gratings in the fiber facet and the SWGs in the glass substrate are presented.

This chapter is organized as follows: The simulation parameters and optimum coupling efficiency results are described for EW coupling. Secondly, the influence of the width of the input light beam on the output far-field intensity pattern is depicted. Thirdly, the effect of a finite number of grating lines in one of the gratings is discussed. Next, misalignment effects are analyzed. Then, the impact of two examples of variations in the glass grating is observed and discussed. Last, conclusions are stated.

4.1 Simulation Set-Up

A Gaussian wave of wavelength 0.65 µm, normally incident on the gratings, was chosen as the illuminating light source, as opposed to a longer, non-visible infrared wavelength to permit visual inspection. The light was TE-polarized (i.e. the electric field
is parallel to the gratings). The first grating was patterned with a 50% duty cycle, i.e. lines of equal width $l_1$ were separated by a distance $d_1 = l_1$; the refractive index was equal to the effective index of a silica fiber ($n_1 \approx 1.456$). The second SW grating was patterned in a 4 µm thick borosilicate glass substrate ($n_2 \approx 1.47$) with 50% duty cycle. The surrounding medium where the field was recovered was air ($n_0 = 1$). The two-dimensional simulation domain had dimensions 320 µm in the x (transverse) direction and 8 µm in the z (propagation) direction, and the minimum mesh size used was 0.02 x 0.02 µm2. The far-field pattern is calculated from the near field, using a wide angle far field transform based on the Fresnel-Kirchhoff diffraction formula [286]. The simulation layout is illustrated in Figure 30.
Figure 31: a) Coupled 200 nm and 500 nm gratings, with 1 µm equivalent period. b) Diffraction orders generated by coupled gratings when $\Lambda_1 = 200$ nm and $\Lambda_2$ is varied between 200 and 600 nm. In this case only the 200 nm - 500 nm pair is not subwavelength and gives rise to a diffraction order at about 40.5°
We performed the CSWGs concept using optical simulations. We observed higher-order diffraction peaks in the far field every time the combination of the two gratings formed a structure with a non-subwavelength period equal to the least common multiple of the periods of the gratings. For example, for a grating pair with periods 200 nm and 500 nm a diffraction order was observed at \(~40.50^\circ\), as illustrated in Figure 31, consistent with the diffraction angle for a period of \(\Lambda = 1000\) nm or 1 \(\mu\)m given by equation (2). Likewise, for a grating pair with periods 300 nm and 400 nm (combined period of 1200 nm or 1.2 \(\mu\)m), we had a diffraction order at 32.8\(^\circ\), and for periods of 300 nm and 500 nm (combined period of 1500 nm or 1.5 \(\mu\)m) we had a first diffraction order at 25.6\(^\circ\) and a second diffraction order at 60.1\(^\circ\).

4.2 Optimization of Gratings Periods and Thicknesses

To obtain the maximum coupling output efficiency from the CSWG system, optimization of the gratings dimensions needed to be performed. The initial grating thickness for the CSWGs was 200 nm, from the result for optimal thickness of glass-to-glass assemblies produced by Rogers, et. al [15]. There was no gap between the gratings. Additionally, the half-width-half-maximum (HWHM) of the input electric field was selected to be 50 \(\mu\)m (FWHM = 100 \(\mu\)m) to cover a large window in a simulation domain of width 320 \(\mu\)m. In an effort to determine the optimal coupled SWG pair, the period of the first grating (etched in the optical fiber) \(\Lambda_1\) and the period of the second SWG \(\Lambda_2\) were both individually varied from 200 nm to 640 nm (gratings still SW to the 650 nm incident source) in 20 nm increments as illustrated in Figure 32.
Higher diffraction orders were observed in the far field every time the combination of the two gratings formed a structure with a non-subwavelength period equal to the least common multiple of the periods of the gratings. The output intensity was normalized to be expressed in dB, as shown in equation (60), to account for the output of the simulated data being expressed in arbitrary units (a.u.):

$$10 \cdot \log_{10} \left( \frac{P_{1st}}{P_{0th}} \right) = P_{dB}. \quad (60)$$

The maximum output intensity was obtained when the first grating period was 580 nm and the second grating period was 560 nm, forming an effective period of 16.24 µm. However, to be able to better differentiate the first order from the other higher diffraction orders, the pair $\Lambda_1 = 560$ nm and $\Lambda_2 = 420$ nm with a smaller effective period of 1.68 µm, illustrated in Figure 33, was selected. This SWG pair produces a diffraction order at 22.76°, which is consistent with the diffraction angle for a period of $\Lambda = 1.68$ µm.
Choosing CSWG periods of $\Lambda_1 = 560 \text{ nm}$ and $\Lambda_2 = 420 \text{ nm}$, the next simulation was performed to optimize the grating thicknesses and produce the maximum output intensity. The thickness of each grating was varied from 100 nm to 600 nm in 100 nm increments. The values of the relative maximum output intensity in dB of each peak are given in Table 4. The highest maximum output intensity was found to be -11.42 dB for the fiber gratings with thickness of 300 nm and a borosilicate glass grating thickness of 400 nm.

From these experiments, the optimum parameters for the gratings etched in the silica fiber are a grating period of 560 nm and a grating thickness of 300 nm. The gratings etched in the borosilicate glass substrate have a grating period of 420 nm and a grating thickness of 400 nm. The next section will focus on the input beam diameter and its effect on the maximum output intensity.

Figure 33: 1.68 $\mu$m equivalent grating period from a 560 nm and 420 nm grating pair
Table 4: First order far-field output intensities of variable grating thicknesses for $\Lambda_1 = 560$ nm – $\Lambda_2 = 420$ nm SWG pair

<table>
<thead>
<tr>
<th>Grating thickness etched in glass substrate</th>
<th>100 nm</th>
<th>200 nm</th>
<th>300 nm</th>
<th>400 nm</th>
<th>500 nm</th>
<th>600 nm</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 nm</td>
<td>-26.95 dB</td>
<td>-24.74 dB</td>
<td>-25.35 dB</td>
<td>-22.80 dB</td>
<td>-27.00 dB</td>
<td>-29.87 dB</td>
</tr>
<tr>
<td>300 nm</td>
<td>-17.75 dB</td>
<td>-13.98 dB</td>
<td>-12.31 dB</td>
<td>-11.42 dB</td>
<td>-14.46 dB</td>
<td>-16.19 dB</td>
</tr>
<tr>
<td>400 nm</td>
<td>-17.11 dB</td>
<td>-13.66 dB</td>
<td>-12.76 dB</td>
<td>-11.52 dB</td>
<td>-14.63 dB</td>
<td>-16.39 dB</td>
</tr>
<tr>
<td>500 nm</td>
<td>-21.11 dB</td>
<td>-18.04 dB</td>
<td>-15.95 dB</td>
<td>-15.78 dB</td>
<td>-17.78 dB</td>
<td>-19.51 dB</td>
</tr>
<tr>
<td>600 nm</td>
<td>-25.86 dB</td>
<td>-25.53 dB</td>
<td>-20.99 dB</td>
<td>-23.23 dB</td>
<td>-23.54 dB</td>
<td>-25.25 dB</td>
</tr>
</tbody>
</table>

4.3 Effect of Beam Width

After optimization of the gratings periods and thicknesses, the effect of the beam width on the coupled gratings was investigated. We first determined the noise floor by running simulations with one subwavelength grating, the borosilicate layer being completely absent. Since a single SW grating allows transmission of only the zeroth order, the lower level of the transmitted signal can be considered noise, and this level did not change for CSWGs. Similarly to the transmitted electromagnetic wave intensity the noise was expressed in dB following the formula:

$$10 \cdot \log_{10} \left( \frac{P_{\text{noise}}}{P_{0th}} \right) = P_{\text{dB}} \cdot (61)$$

A minimum HWHM of 4 µm (FWM = 8 µm), was necessary for a defined separation between the diffraction and noise floor. For larger beam widths, the noise level
stayed at a minimum below -160 dB for HWHM up to 30 µm (FWHM = 60 µm) as visible in Figure 34. A close-up between HWHM 26 µm and 34 µm revealed that the minimum was in fact 28 µm (FWHM = 56 µm). The level rose for HWHM larger than 28 µm, due to the stronger contribution of secondary maxima [287].

Figure 34: Effect of Beam Width on CSWGs with grating periods $\Lambda_1 = 560$ nm and $\Lambda_2 = 420$ nm with HWHM varied from 10 µm to 100 µm in 10 µm increments and from 100 µm to 200 µm in 50 µm increments, and on single subwavelength gratings (sw) with grating period $\Lambda_1 = 560$ nm

From the result presented in this section, it can be concluded that 8 µm is the minimum beam diameter that will allow distinguishing between two diffraction orders, but with beams wider than 56 µm contrast will be diminished in the far-field pattern. In the next section, the effects of having a finite number of grating lines will be presented.
4.4 Effect of the Number of Grating Lines

The envisioned device has the first grating of the CSWG pair FIB-milled on the facet of an optical fiber. As a result, there are a maximum number of grating lines that can be patterned. The next simulations presents the effect the number of grating lines has on the output of the CSWG pair when the first grating with period 560 nm and thickness 300 nm has a finite number of lines and the second grating with period 420 nm and thickness 400 nm an “infinite” number of lines. Infinite denotes that the second grating was so much larger than the first one and that any effect due to its size limitations became negligible. Each line was represented by an integer number m, m = 0 being the center line, m = ±1 the first lines to the left and to the right of the center line, and so on, following the same nomenclature as for diffraction orders. The total number of lines was thus N = 2m + 1. The wavelength of the input source was 650 nm with a HWHM of 28 microns.

With a 0 nm gap between the gratings, the first order diffraction peak started to emerge as dominant in the region for m = 7 (N = 15), as seen in Figure 35(a). In the coupled gratings system this gives five effective periods. In practical applications, it is not easy to bring the two gratings into contact without a gap between them, so the two gratings were also placed in proximity with a gap of 300 nm between them. With the 300 nm separation, the first order peak was dominant for m = 11 (N = 23), with lower maximum intensity, as shown in Figure 35(b). The noise level also decreased significantly for large m to reach a bottom below -160 dB when approaching m ≈ 300 (N ≈ 601) where the number of lines can be considered infinite for practical purposes as seen for the 0 nm gap in Figure 36.
The minimum number of 15 grating lines on the fiber facet established, one more consideration was the misalignments inherent to a multi-component assembly. They are discussed in the next section.

Figure 35: Far-Field Diffraction Patterns: a) Far-field diffraction patterns for small numbers of grating lines in the first grating of a coupled pair with no gap between them. b) Far-field diffraction patterns for small numbers of grating lines in the first grating of a coupled pair with a 300 nm gap between them.

Figure 36: Far-field diffraction patterns for large numbers of grating lines in the first grating of a coupled pair with no gap between them.

Figure 37: Far-field diffraction patterns for large numbers of grating lines in the first grating of a coupled pair with no gap between them.
4.5 Effect of Rotational Misalignment

In a physical environment, it can be a challenge to perfectly align the light source to first grating #1 and grating #1 to grating #2. When the first grating is written directly on the fiber facet, the fabrication process eliminates misalignment of the beam, since the grating remains at a fixed position relative to the incident beam. However, the cylindrical shape of the fiber might give rise to a slight rotation $\gamma$ of the fiber grating with respect to the second grating, as illustrated in Figure 37, where the cases of perfect alignment (0° rotation) and 15° rotation of the fiber grating are shown. The dominant moiré fringes created by the superposition of two gratings with close periods are visible in Figure 37(b).

Figure 37: Perfect rotational alignment between fiber and borosilicate glass gratings. (b) 15-degree rotation of the fiber grating with respect to the borosilicate glass grating, giving rise to moiré fringes at an angle $\zeta$.

When the spacing between the moiré fringes is large, these fringes will constitute a new effective non-subwavelength grating for the wavelength in use and will result in a
different far-field diffraction pattern. The orientation of the fringes follows the intersection points of the two gratings, and the diffraction orders must deviate from the horizontal axis by this same angle. The fringe angle $\zeta$ and period $\Lambda_f$ can be determined as solved in [288]:

$$\sin \zeta = \frac{\Lambda_2 \sin \gamma}{\sqrt{\Lambda_1^2 + \Lambda_2^2 - 2 \cdot \Lambda_1 \Lambda_2 \cos \gamma}} \tag{62}$$

and

$$\Lambda_f = \frac{\Lambda_1 \Lambda_2}{\sqrt{\Lambda_1^2 + \Lambda_2^2 - 2 \cdot \Lambda_1 \Lambda_2 \cos \gamma}} \tag{63}$$

In order to verify the effect of the fiber rotation i.e. of the moiré pattern on the output of CSWGs, a 3D simulation environment was necessary to represent movement around the propagation axis ($z$). To avoid reaching the memory limit of the computer system the FDTD computation domain was limited to a rectangular parallelepiped $L \times W \times H = 6 \, \mu m \times 20 \, \mu m \times 20 \, \mu m$. The fiber designed with OptiFDTD emulated the last micron at the output extremity of a silica fiber with core index $n_{co} = 1.45653$ and cladding index $n_{cl} = 1.45187$ at the wavelength $\lambda_0 = 650 \, \text{nm}$, in which is propagating the LP01 mode or fundamental (lowest order) mode of the fiber. The core diameter was 8.2 $\mu m$. The cladding diameter would theoretically be 125 $\mu m$ but since this dimension is much larger than the domain considered in the simulation, the diameter was chosen such that it just covered the domain. At the operating wavelength the LP modes are well confined in the core and the smaller cladding did not change the fiber modes behavior. The fiber grating
covered an area of 10 µm x 10 µm at the center of the fiber output facet. The fiber grating period was 560 nm with a fill factor of 50% and an optimal thickness of 300 nm. The grating on glass (n_g = 1.47) covered the entire domain, with a period of 420 nm, a fill factor of 50% and an optimal thickness of 400 nm. The periods of the gratings gave an effective period of 1.68 µm. With 20 grating lines on the fiber 5 whole effective periods were present for discernible first orders. The thickness of the glass substrate was 4 µm. The resulting output in dB is shown in Figure 38 for perfectly aligned gratings (no rotation), where the bright red represents 0 dB and is the greatest output intensity. The first orders were centered at a diffraction angle \( \theta \approx 23^\circ \), matching the calculations for a 1.68 µm equivalent period.

![Figure 38: Far-field output intensity map](image-url)
The calculation results for the fringe angles with respect to the vertical axis, the simulated fringe angles given by the first orders position with respect to the horizontal axis, the calculated fringe spacing and the diffraction angle $\theta$ of the first diffraction order are given in Table 5, with the parameters mentioned above, for different angles $\gamma$ between the gratings. Table 5 suggests that for rotation angles of $40^\circ$ and higher, the fringe pattern becomes subwavelength for the operating wavelength and does not generate higher orders in the far field, which was verified in the simulations. The simulated far-field pattern displayed a rotation with respect to the horizontal axis that followed the calculated fringe angles, with a small difference attributed to the precision of the simulation cell size (in particular, faint first orders were still discernible for $\gamma = 40^\circ$ at large diffraction angles).

<table>
<thead>
<tr>
<th>Rotation angle $\gamma$ (deg)</th>
<th>Calculated fringe angle $\zeta_c$ (deg)</th>
<th>Simulated fringe angle $\zeta_s$ (deg)</th>
<th>Calculated fringe spacing $\Lambda$ (µm)</th>
<th>Calculated diffraction angle $\theta$ (deg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.68</td>
<td>22.76</td>
</tr>
<tr>
<td>5</td>
<td>14.49</td>
<td>$\sim$-16</td>
<td>1.61</td>
<td>23.84</td>
</tr>
<tr>
<td>10</td>
<td>26.48</td>
<td>$\sim$-29</td>
<td>1.44</td>
<td>26.87</td>
</tr>
<tr>
<td>15</td>
<td>35.16</td>
<td>$\sim$-38</td>
<td>1.25</td>
<td>31.44</td>
</tr>
<tr>
<td>20</td>
<td>40.99</td>
<td>$\sim$-42</td>
<td>1.07</td>
<td>37.25</td>
</tr>
<tr>
<td>25</td>
<td>44.70</td>
<td>$\sim$-44</td>
<td>0.93</td>
<td>44.22</td>
</tr>
<tr>
<td>30</td>
<td>46.94</td>
<td>$\sim$-46</td>
<td>0.82</td>
<td>52.60</td>
</tr>
<tr>
<td>35</td>
<td>48.13</td>
<td>$\sim$-47</td>
<td>0.73</td>
<td>63.39</td>
</tr>
<tr>
<td>40</td>
<td>48.57</td>
<td>$\sim$-47</td>
<td>0.65</td>
<td>-</td>
</tr>
<tr>
<td>45</td>
<td>48.47</td>
<td>-</td>
<td>0.59</td>
<td>-</td>
</tr>
<tr>
<td>50</td>
<td>47.97</td>
<td>-</td>
<td>0.54</td>
<td>-</td>
</tr>
<tr>
<td>55</td>
<td>47.15</td>
<td>-</td>
<td>0.50</td>
<td>-</td>
</tr>
<tr>
<td>60</td>
<td>46.10</td>
<td>-</td>
<td>0.47</td>
<td>-</td>
</tr>
<tr>
<td>65</td>
<td>44.86</td>
<td>-</td>
<td>0.44</td>
<td>-</td>
</tr>
<tr>
<td>70</td>
<td>43.47</td>
<td>-</td>
<td>0.41</td>
<td>-</td>
</tr>
<tr>
<td>75</td>
<td>41.95</td>
<td>-</td>
<td>0.39</td>
<td>-</td>
</tr>
<tr>
<td>80</td>
<td>40.34</td>
<td>-</td>
<td>0.37</td>
<td>-</td>
</tr>
<tr>
<td>85</td>
<td>38.64</td>
<td>-</td>
<td>0.35</td>
<td>-</td>
</tr>
<tr>
<td>90</td>
<td>36.87</td>
<td>-</td>
<td>0.34</td>
<td>-</td>
</tr>
</tbody>
</table>
The resulting far-field pattern with $\gamma = 5^\circ$ rotation, is shown in Figure 39 and can be compared to the no-rotation case in Figure 38.

Figure 39: Far-field pattern with fringe angle 16o resulting from the presence of a 5° fiber rotation

4.6 Variations in Glass Grating

To create a unique signature, it was important to observe the effect small variations in the second grating (etched in borosilicate glass) would have on the far-field pattern. The objective was to detect and observe a diffraction pattern that would be different for each grating pair. In the second grating, while each line remained centered at its original location, maintaining the effective grating period, they had a random width taken within a
uniform interval centered at the original line width. In Figure 40a, the line width was varied between 147 nm and 273 nm, which represent a 30% variation on each side of the center line width, 210 nm. In Figure 40b, where is shown the far-field patterns of a regular and two varied CSWGs it can be seen how this line width deviation introduced variations in the output of two instances of varied coupled gratings while the diffraction peaks stayed visible and were still located at the same angles. The first order maximum remained defined in both device samples and the signature unique to a specific sample. The second maximum adjacent to the first order was a combined consequence of the presence of the gap and the small beam width.

The concept of the CSWGs signature having been modeled with random variations, one more consideration was the ease of fabricating and testing a specific instance of varied gratings. In order to be able to compare simulations and tests results, two instances were designed with a planned pattern so that the fabricated CSWGs would be the same as the simulated ones.

The first CSWGs featured a series of larger lines of width 1.05 µm separated by a periodic distance of 14.7 µm, slightly larger than the width covered by the fiber gratings. It was hypothesized that starting with the fiber centered on one “defect” and moved in steps to the next defect, the output intensity would be the same at those two end points and there would be mirror symmetry of maximum intensity between positive and negative first orders for every two positions equidistant from the center point between two defects. The concept is illustrated in Figure 41(a) and the symmetric distribution of maximum intensities in Figure 41(b) and Figure 41(c). The points are connected better visibility.
Figure 40: a) Line width variation in the second grating of a coupled pair, between 147 nm and 273 nm, interval representing a 30% variation on each side of the center line width, 210 nm. b) Far-field pattern for 30% line width variation. The pattern for a regular grating is also given for reference.
Figure 41: a) Mirror symmetry positions around periodic defects. b) and c) Symmetric distribution of maximum intensities
Figure 42: a) Similar positions in periodically varied grating (period 13.86 µm). b) Maximum output intensities are the same for a first diffraction order at two similar positions (0 µm and 13.86 µm)
In the second CSWGs, the line widths were varied in ascending order from 150 nm to 210 nm to 270 nm over a period of 13.86 µm. In this case as well the maximum output intensity would be the same for a first diffraction order at two similar positions (over a length of 13.86 µm). This is illustrated in Figure 42.

4.7 Conclusion

The effect of beam size, finite number of lines, rotational misalignment and grating variations on coupled subwavelength gratings was investigated in this chapter. After establishing that the effective period given by the combination of the periods of the grating pair must be non-subwavelength for transmission of higher diffraction orders to take place, the characteristic parameters of regular infinite gratings, periods and thickness, were optimized, for a wavelength of 650 nm. The best dimensions were found to be a period of 560 nm for the first grating made of silica and 420 nm for the second borosilicate glass grating. The size of the input light beam had to be a HWHM of at least 7 µm to allow discernible higher transmission orders, and a HWHM of 28 µm for minimum noise. At least 15 lines needed to be present on the fiber facet. Grating rotation due to milling the first grating in the CSWG pair directly on a fiber facet, resulted in a rotation of the far-field pattern, corresponding to the rotation angle of moiré fringes.
CHAPTER V: Gratings Fabrication

Standard use of focused ion beam (FIB) and electron beam lithography (EBL) were introduced in Chapter III. Here, we will describe how they were applied to the fabrication of gratings on fiber facet and gratings on glass substrate. Both material being dielectric, charging effect had to be addressed.

5.1 Gratings on Fiber Facet

A length of 25 mm was stripped out of a 60-cm long Thorlabs SMF-28 optical fiber, cleaned with Acetone and Isopropyl Alcohol (IPA) and cleaved with an Ericsson EFC11-4 fiber cleaver to leave a flat facet at the end of bare fiber length of 1 mm, as can be observed in Figure 43(a) obtained from the scanning electron microscope (SEM) imaging system of the JEOL JIB-4500 focused ion beam (FIB) machine in the FIU Advanced Materials Engineering Research Institute (AMERI). To avoid charging, the fiber tip was sputtered with a 3-nm thick layer of gold, using a Pelco SC-7 auto sputter coater. The pressure was brought down to 0.01 mbar, and sputtering lasted 50 seconds at 30 mA. In order to have the fiber facet facing to ion beam column of the FIB machine, the bare tip of the fiber was affixed using copper tape to the top of a custom-made mount angled at 52° to match the FIB column. The remaining of the fiber strand was folded around the mount and secure with more copper tape. Multiple fibers can be arranged on a single mount, as shown in Figure 43(b).

The gratings were milled by FIB at the center of the fiber facet with the following parameters:
Table 6: Parameters for FIB milling on fiber facets

<table>
<thead>
<tr>
<th>Number of lines</th>
<th>Width of lines</th>
<th>Length of lines</th>
<th>Width of spaces</th>
<th>Beam current</th>
<th>Dose</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>280 nm</td>
<td>15 µm</td>
<td>280 nm</td>
<td>500 pA</td>
<td>1.5 nC/µm²</td>
</tr>
</tbody>
</table>

The top view and cross section of the resulting gratings on Fiber #1 are pictured in Figure 44. The trapezoidal shape of the lines is attributed to a combination of redeposition, ion beam profile and dependency of the sputter yield on incidence angle [271, 289-292].

Figure 43: a) Stripped and cleaved fiber mounted in JEOL FIB machine. b) Fibers mounted in preparation for FIB
5.2 Gratings on Glass Substrate

The gratings were designed in Juspertor’s LayoutEditor. Four identical rows, made of regular subwavelength gratings along with what would be their non-subwavelength equivalent when coupled with a grating of period 560 nm and the three simulated varied gratings, were drawn to fit inside a 4-inch wafer. Each grating covered an area of 500 µm x 500 µm. The complete layout, with dimensions, is depicted in Figure 45(a) and a close-up on one varied grating is shown in Figure 45(b).
Figure 45: a) Gratings design in LayoutEditor. b) Varied grating design

The gratings were subsequently patterned using a JEOL JBX-6300FS electron beam lithography (EBL) system. A glass substrate was spin coated with ZEP-520. After the
ZEP520 was spun on the glass substrate, a thin layer of ESPACER was spun on the ZEP520 to dissipate the charge buildup during EBL as shown in Figure 46.

![Figure 46: EBL process flow on a glass substrate with an ESPACER charge dissipation agent and ZEP photo resist](image)

The sample was then exposed with the EBL grating pattern and rinsed in de-ionized water to remove the ESPACER, and blown dry with nitrogen. The sample was developed in amyl acetate to completely remove the ZEP520 that was exposed during the e-beam patterning. The ZEP520 resist was used as a mask layer to etch the gratings 400 nm deep into the glass substrate using a STS glass etcher. The wafers were cleaned in acetone and methanol.

To avoid charging effect during scanning electron microscope (SEM) imaging, the first row of the sample was sputtered with a gold-palladium alloy. The deposition time was 40s, which led to a thickness of 12 to 16 nm. The resulting SEM images for a non-subwavelength grating of period 1.68 µm, a regular subwavelength of period 0.42 µm and the varied subwavelength grating in Figure 42(a) and Figure 45(b) are shown in Figure 47. Here again, in the cross sections in Figure 47(b) and (d) the gratings show a trapezoidal profile, result of process fabrication steps, i.e., e-beam lithography and RIE etching.
Figure 47: SEM pictures of gratings fabricated on glass substrate. a) Top view of regular non-subwavelength grating. b) Cross section of regular non-subwavelength grating. c) Top view of regular subwavelength grating. d) Cross section of regular subwavelength grating. e) Top view of varied subwavelength grating
CHAPTER VI: Tests, Results and Discussion

Testing and verification of the tamper-evident system was first confirmed from the simulation results in Chapter IV. In this section, an explanation of the test setup used and a comparison of the output intensity from the simulation results and the measured output intensity from the evanescent wave coupling of the SWG and the grating fiber are presented. The SWG etched into the facet of the optical fiber was brought into contact, which represents a 0 µm gap separation, with the SWG on the glass substrate. This resulted in far-field diffraction being observed. As the grating samples lost contact and began to separate, the far-field diffraction pattern became dimmer and eventually disappeared. The overall total system assessment is described in detail, and future work including unique identification is introduced.

6.1 Test Set-Up

The final test set-up is depicted in Figure 48.

![Figure 48: Complete test set-up for evanescent coupling]
6.1.1 Light Sources

In the test setup, two light sources were used. The first one was used for rotational alignment of the beam and the other was used as the incident source for the SWG and fiber grating pair.

The first source was a 5 mW green ($\lambda = 532$ nm) laser that was coupled to the optical fiber via a Thorlabs ST1XY-S XY translation mount mounted vertically on a post. The translation mount allows the user to adjust the beam position, further centering the beam in the fiber core. The laser was secured in horizontal position by a lens holder and a retaining ring inside the holder, as illustrated in Figure 49.

The second light source that was previously shown in the final set-up in Figure 48 was a 10 mW red ($\lambda = 650$ nm) Thorlabs L650P007 diode laser driven by a LDC201CU.
current controller, and coupled to the optical fiber via focusing lenses and a Thorlabs ST1XY-S XY translation mount mounted vertically on a post. The fiber input was affixed to the translation mount via a FC-PC fiber connector that was connected to a fiber adapter with external plate screwed into the translation mount. These different lens and translations mounts are used for maximizing the amount of light that is transmitted through the optical fiber.

6.1.2 Fiber and glass substrate mounting

The gratings that were etched into the optical fiber were written using the focused ion beam (FIB). The grating dimension on the fiber had a 15 µm field size with a grating of period 560 nm and 30 individual lines. The fiber was then secured using a strong tape and placed in a groove milled in an Aluminum chuck. The chuck was attached to the Thorlabs Max302 flexure translation stage. The fiber was extended beyond the stage to ensure that it touched the SWG sample in the glass substrate. As previously mentioned, the green light source was used to determine the beam alignment, it was also used to ensure that the diffraction orientation followed the same convention as the those in the simulations. The glass substrate was fixed using a Thorlabs FH2 filter holder attached on top of a 2-inch pole. Using a Thorlabs RA180 90o clamp, the 2-inch pole was mounted perpendicularly on a 6-inch horizontal post attached in turn via a Thorlabs RA90 90o adapter to a third, vertical post. This arrangement avoided having a vertical post base between the flexure stage holding the fiber and the photodetector, allowing close positioning of fiber, glass substrate and photodetector. The fiber longitudinal axis was
perpendicular to the plane of the filter holder. The grating lines on the glass substrate were vertical, allowing diffraction along a horizontal line.

6.1.3 Readout

The output light was recorded using a Thorlabs SC130C photodiode power sensor. The photodiode was attached on a Newport 562 series x-y-z stage that allowed for accurate movements to center the output onto the photodiode. Additionally, the photodiode was connected to the Thorlabs PM100USB power and energy meter that communicated via USB for real-time data acquisition.

To verify the accuracy of the photodetector output, the laser was focused directly into the photodetector. A constant power input was set to 10 mW and the photodetector output showed an output value of 18 V. Additionally, when the laser is normally incident upon the glass, without gratings, the transmitted output power was measured to be 15.86 V. This decrease in output intensity is a within 5% of the expected value due to Fresnel reflections at the air:glass and glass:air interfaces (4%).

6.2 Testing

6.2.1 Gratings alignment

The first step in preliminary testing with the fiber grating was to ensure that the grating lines on its facet were parallel to the lines of the glass grating and that the fiber diffraction orders were within the transverse horizontal (x) distance covered by the x-y-z stage supporting the photodetector. For that purpose the green laser pointer was used at the input of the optical fiber, and a white round checkered screen of 1 inch diameter (to
match the external threader centered on the photodetector) was placed in front of the photodetector, facing the fiber output. A dot at the center of the circle marked the location of the photodetector (Figure 50). Using the 532 nm laser, the grating period on the fiber is non-subwavelength to this source. Therefore, higher diffraction orders were visible on the projection screen (Figure 51). The fiber was rotated until all orders 0 and +/-1 fell on a horizontal line. The distance between fiber and screen was adjusted until with the fiber fixed, the photodetector was able to travel completely from left to right without the first higher orders leaving the checkered screen. The x-knob marking at which the photodetector was directly in front on the fiber (detecting the 0th order at its maximum) was noted. The vertical (z-) position of the photodetector was also adjusted for maximum output. A mirror was then placed in placed of the screen to verify perpendicularity of the fiber with respect to the photodetector plane. Finally, a vertical 200-micron slit was placed in front of the photodetector to ensure isolation of the different diffractions orders. The actual test set up is pictured in Figure 52.

Figure 50: Checkered screen for fiber alignment with photodetector
With the gratings aligned, the grated fiber facet was positioned to touch the glass grating by movements of the flexure stage (Figure 53). This was visually observed using the Caltex long-range microscope with a Lumenera camera that could record video and images to a computer.

Figure 51: With the 532 nm laser, the grating period on the fiber is non-subwavelength to the source. Therefore, higher diffraction orders were visible on the projection screen.

Figure 52: Actual test set up
6.2.2  Tests with large gratings

A non-subwavelength grating of period 1680 nm is the equivalent of two subwavelength gratings of periods respectively 560 nm and 420 nm. Such a grating was used to ascertain the positions at which the first order diffractions would be captured by the photodetector, since the diffraction angles for this equivalent grating would be the
same as for the CSWGs. The red light source ($\lambda = 650$ nm) Thorlabs L650P007 was used. The photodetector was placed at a distance of 10 mm from the glass grating, and moved along the x axis so as to scan the diffraction pattern. The peaks of the +1 and -1 orders, seen on Figure 54, were at the 4 mm and -4 mm positions respectively, consistent with a diffraction angle of 22.76°. The same was repeated with a non-subwavelength grating of period 3360 nm, equivalent to subwavelength gratings of periods 560 nm and 480 nm respectively.

6.2.3 Evanescent coupling

The evanescent wave coupling was observed by placing the SWG on the fiber into contact with the SWG in the glass substrate. While scanning the output intensity of the CSWG pair with the photodector, the diffraction pattern was visible on the opaque screen, as seen in Figure 55 for a 560 nm – 480 nm pair of SW gratings, and consistent with simulations, as illustrated in Figure 56.

Figure 55: Observed pattern resulting from evanescent coupling
However, there were instances where measurements were not observed. This is a result of the normal incidence. To measure the higher diffraction orders at their maximum intensity, the incident angle of the higher diffraction orders needed to be normally incident on the active area of the photodetector. As a result, an 180° protractor was placed on the table, its origin at the level of the point of incidence, as illustrated in Figure 57. The photodetector was placed on the protractor arc at the angles corresponding to diffraction orders 0, -1 and +1, successively. The slit was removed from the photodetector, as the distance between CSWGs and photodetector allowed complete separation of each order. Additionally, it was ensured that the spot size of the diffraction orders was smaller than the active area of the photodetector. Tests were conducted with glass gratings of period 420 nm, and 480 nm for comparison. Two grating samples were
used for each period. Although the absolute output values varied due to changes in fiber length and bending, and quality of the coupling between the subwavelength gratings (gap separation and angle between coupled gratings), the relative values of the ±1st orders remained within a standard deviation of less than 2 dB, as can be seen in Table 7 and Table 8.

Table 7: Output intensity in diffraction orders captured by photodetector with 560 nm – 420 nm grating pair

<table>
<thead>
<tr>
<th>Unit</th>
<th>0th order</th>
<th>-1st order</th>
<th>+1st order</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>W</td>
<td>dB</td>
<td>W</td>
</tr>
<tr>
<td>Sample 1, test 1</td>
<td>0.135E-6</td>
<td>1</td>
<td>1.600E-9</td>
</tr>
<tr>
<td>Sample 1, test 2</td>
<td>0.124E-6</td>
<td>1</td>
<td>0.900E-9</td>
</tr>
<tr>
<td>Sample 1, test 3</td>
<td>0.124E-6</td>
<td>1</td>
<td>0.700E-9</td>
</tr>
<tr>
<td>Sample 2, test 1</td>
<td>0.126E-6</td>
<td>1</td>
<td>0.850E-9</td>
</tr>
<tr>
<td>Sample 2, test 2</td>
<td>1.100E-6</td>
<td>1</td>
<td>17.00E-9</td>
</tr>
<tr>
<td>Standard deviation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 57: The photodetector is placed at a diffraction angle to capture the higher order at its maximum intensity
Table 8: Output intensity in diffraction orders captured by photodetector with 560 nm – 480 nm grating pair

<table>
<thead>
<tr>
<th></th>
<th>Unit</th>
<th>0° order</th>
<th>-1° order</th>
<th>+1° order</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>W</td>
<td>dB</td>
<td>W</td>
<td>dB</td>
</tr>
<tr>
<td>Sample 1, test 1</td>
<td>1.000E-6</td>
<td>1</td>
<td>12.00E-9</td>
<td>-19.21</td>
</tr>
<tr>
<td>Sample 1, test 2</td>
<td>0.890E-6</td>
<td>1</td>
<td>17.00E-9</td>
<td>-17.19</td>
</tr>
<tr>
<td>Sample 1, test 3</td>
<td>0.400E-6</td>
<td>1</td>
<td>8.00E-9</td>
<td>-16.99</td>
</tr>
<tr>
<td>Sample 2, test 1</td>
<td>0.600E-6</td>
<td>1</td>
<td>7.80E-9</td>
<td>-18.86</td>
</tr>
<tr>
<td>Sample 2, test 2</td>
<td>0.559E-6</td>
<td>1</td>
<td>4.20E-9</td>
<td>-21.24</td>
</tr>
<tr>
<td>Standard deviation</td>
<td></td>
<td></td>
<td>1.73</td>
<td>1.84</td>
</tr>
</tbody>
</table>

6.3 Modeling and Measurements Comparison

Far field diffraction was observed from evanescent wave coupling of two subwavelength gratings with different grating periods, fabricated on a fiber facet and in a glass substrate. The grating dimensions were optimized to achieve maximum output in
the +1 and -1 diffraction orders. From SEM analysis and as mentioned in Chapter V, the shapes and dimensions of the fabricated gratings had changed from the profile of the simulated gratings. New simulations were therefore conducted to match the characteristics obtained from the SEM inspection, as shown in Figure 58.

The simulations indicated that there was a change in output intensity from the original grating design to the re-simulated grating as seen in Figure 59. There is a decrease from two- to three-dimensional simulations as well, which highlights further the effect of finite dimensions (in this case, finite length of the grating lines) on performance.

![Figure 59: Simulation output intensity results for 2D and 3D original simulation layout and re-simulation layout from SEM analysis](image_url)
Figure 60: Simulation and experimental results for re-simulated CSWGs with different gap separations a) 560 nm – 420 nm pair b) 560 nm – 480 nm pair
A few nanometers separation is often present between coupled gratings even in the best alignment situation. Therefore data points from Table 7 and Table 8 are plotted in Figure 60 along with re-simulation results showing the dependence of the output intensity on grating separation. The experimental results remained, with acceptable error, close to the re-simulated 3D coupled gratings within a separation between gratings of 200 nm. The higher value of -16dB obtained for the +1st order of the 560 nm – 420 nm grating pair is attributed to rougher alignment at the beginning of the experiment.

6.4 Conclusions and Future Work

Near-field evanescent wave coupling between a SWG on the core of an optical fiber facet and a SWG etched into a glass substrate was demonstrated for the first time in this dissertation, using a 0.65 μm red semiconductor laser. The optimal parameters were determined and the limitations imposed by the fiber geometry established. Effects of variations introduced in the glass grating were also explored. It was successfully verified that the recorded output adequately matched simulated results.

Two different grating fabrication methods were employed during this work. Subwavelength gratings with 560 nm period were successfully demonstrated using focused ion beam milling on a fiber facet and subwavelength gratings with different periods were fabricated using electron beam lithography.

The effect of variations in the grating line width were studied for the creation of a signature, and the next step is to test prototypes of varied CSWGs and verify the repeatability of the signature of a given “fingerprinted” grating when integrity of the
protected device is assumed. A corresponding test setup will be used to demonstrate the concept and the results will be compared to those obtained from the simulations.

The technology of CSWGs with optical fiber for tamper evidence application demonstrated in this dissertation will not only allow to overcome challenges in the testing of devices that are complete with packaging, but it will also assist in increasing production yield by ensuring chip integrity.
References


<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Conference/Source</th>
<th>Pages</th>
</tr>
</thead>
</table>


VITA

ANGE MARIE PATRICIA FIEVRE

Born, Port-au-Prince, Haiti

1997-2003    B.S., Electronic Engineering
Université d'Etat d'Haïti
Port-au-Prince, Haiti

2004-2005    Teaching Assistant
Florida International University
Miami, Florida

The Chancellor's List

2004-2006    M.S., Computer Engineering
Florida International University
Miami, Florida

Latin American and Caribbean Center (LACC) scholarship

2006-2015    Doctoral Candidate
Florida International University
Miami, Florida

2008    Electrical Engineering Intern III
Ball Aerospace and Technologies Corp.
Westminster, Colorado

2009    Electrical Engineering Intern
General Electric Global research Center
Niskayuna, New York

2010    SPIE Educational Scholarship

2012-2014    McKnight Doctoral Fellowship

PUBLICATIONS AND PRESENTATIONS


