A Structure for Protection of Security-Sensitive ICs against Attacks through Silicon Backside

vorgelegt von
M. Sc.
Elham Amini
ORCID: 0000-0002-4580-4243

an der Fakultät IV – Elektrotechnik und Informatik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades
Doktor der Ingenieurwissenschaften
- Dr.-Ing. –

genehmigte Dissertation

Promotionsausschuss:

Vorsitzender: Prof. Dr. Roland Thewes
Gutachter: Prof. Dr. Christian Boit
Gutachter: Prof. Dr. Bernd Szyszka
Gutachter: Prof. Dr. Jean-Pierre Seifert
Gutachter: Prof. Dr. Navid Asadi, University of Florida

Tag der wissenschaftlichen Aussprache: 26. Juni 2020
Berlin 2021

Helmholtz
Research
School on
Security Technologies

This dissertation was started as a part of Helmholtz Research School on Security Technologies (HRSST) and supported by this school.

Dedicated to my family

Abstract

Security sensitive integrated circuits (ICs) are subject to hardware attacks on secure data. In the past few years, optical signal tracking methods accessing the IC through the chip backside have become the most successful attack risks.

Modern ICs are equipped with various hardware and software countermeasures to protect secret data and intellectual property (IP) against known attacks. These countermeasures include protective mesh layers, different sensors, shields, and physically unclonable functions (PUFs). However, the chip backside is still exposed, and proper and affordable protection of the IC backside against focused ion beam (FIB) and optical attacks is missing. Accordingly, the available countermeasures can be circumvented by attacks through the silicon back surface.

This work presents, realizes and develops an efficient and cost-effective structure to protect ICs against hardware attacks through the chip backside. Since there is no cost-efficient way to connect the backside to the frontside electrically, a proper protection structure for the backside must be based on optics. The structure presented here is an optically active thin film that is deposited on the IC back surface. The integrity of the layer is checked by an optical signal generated and detected inside the chip using IC elements. The protective layer is opaque to the infrared light and provides an angle-dependent reflectivity. Thus, the laser light cannot penetrate the IC, and the photon emission of the IC structure cannot leave the IC through the silicon backside. In the developed protection method, the IC structures are administrated as a light-emitting device and light-sensing devices. A p-n junction is forward-biased to emit an optical signal in all directions toward the IC backside. The light reflected from the IC backside is absorbed by several reverse-biased p-n junctions (drain or source of the transistors), creating a photocurrent. The layer changes the intensity of the reflected light depending on the angle of incidence of the light. Therefore, the photocurrent of the detectors is a signature of the layer. If the layer is damaged or removed, the signal of the detectors will change. Then, the device will not be able to confirm the integrity of the layer. Subsequently, the secret data stored on the device will be destroyed. In order to achieve an efficient protection structure, parameters including optical signals, the light emitter, detectors, the protection layer, and the position of the structures are optimized together. In this work, two optically active thin films that are qualified for this purpose are designed and produced by the sputtering method. The layers are characterized by ellipsometry and the Automated reflectance/transmittance analyzer (ARTA). The concept of the protection mechanism is evaluated by electrical measurements on the IC structure. The photocurrent of the detectors is analyzed when the layer is deposited on the IC backside and when the layer is removed. The results have confirmed the effect of the layer on the photocurrent of the detectors. Hence, any harms to the layer can be detected by electrical measurements on the IC circuit. This work also discusses the

advantages and drawbacks of the protection mechanism, and possibilities for its application are examined.

These investigations lead to the conclusion that the protection structure, after optimization of the critical parameters, becomes a comprehensive countermeasure. It would be a very low-cost process and capable of preventing both physical and optical attacks through the chip back surface. This protection structure can be used for all types of security-sensitive ICs with different size, technology, and bulk thickness.

Zusammenfassung

Sicherheitsempfindliche integrierte Schaltkreise (ICs) sind Hardware-Angriffen auf sichere Daten ausgesetzt. In den letzten Jahren sind optische Signalverfolgungsmethoden, die über die Chip-Rückseite auf den IC zugreifen, zu den größten Angriffsrisiken geworden.

Moderne ICs sind mit verschiedenen Hardware- und Software-Gegenmaßnahmen ausgestattet, um geheime Daten und geistiges Eigentum (IP) vor bekannten Angriffen zu schützen. Diese Gegenmaßnahmen umfassen Gitterschichten, verschiedene Sensoren, Abschirmungen und Physically Unclonable Functions (PUFs). Die Chiprückseite ist jedoch immer noch ungeschützt, und es fehlt ein angemessener und erschwinglicher Schutz der Chip-Rückseite gegen fokussierte Ionenstrahlen (FIB) und optische Angriffe. Dementsprechend können alle verfügbaren Gegenmaßnahmen mittels Angriffen durch die Silizium-Rückseite umgangen werden.

In dieser Arbeit wird eine effiziente und kostengünstige Struktur zum Schutz von ICs gegen Hardware-Angriffe durch die Chip-Rückseite vorgestellt, realisiert und entwickelt. Da es keine kostengünstige Möglichkeit gibt, die Rückseite mit der Vorderseite elektrisch zu verbinden, muss eine geeignete Schutzstruktur für die Rückseite auf optischen Prinzipien basieren. Die hier vorgestellte Struktur ist ein optisch aktiver Dünnfilm, der auf der IC-Rückseite aufgebracht wird. Die Intaktheit der Schicht wird durch ein optisches Signal überprüft, das im Inneren des Chips mit Hilfe von IC-Elementen erzeugt und detektiert wird. Die Schutzschicht ist für Infrarotlicht undurchlässig und bietet eine winkelabhängige Reflektivität. Dadurch kann das Laserlicht nicht in den IC eindringen, und die Photonenemission der Schaltung kann den Chip nicht durch die Silizium-Rückseite verlassen. Für die entwickelte Schutzmaßnahme werden IC-Strukturen als lichtemittierende und lichtempfindliche Bauelemente verwendet. Ein p-n-Übergang wird in Vorwärtsrichtung vorgespannt, um ein optisches Signal in alle Richtungen zur IC-Rückseite zu emittieren. Das von der IC-Rückseite reflektierte Licht wird von mehreren in Sperrichtung vorgespannten p-n-Übergängen (Drain oder Source der Transistoren) absorbiert, wodurch ein Fotostrom erzeugt wird. Die Schicht verändert die Intensität des reflektierten Lichts in Abhängigkeit vom Einfallwinkel des Lichts. Daher stellt der Fotostrom der Detektoren eine Signatur der aufgebrachten Schicht dar. Wenn die Schicht beschädigt oder entfernt wird, ändert sich das Signal der Detektoren und folglich kann die Integrität der Schicht nicht mehr bestätigt werden. In der Folge kann der IC alle auf dem Gerät gespeicherten vertraulichen Daten löschen. Um eine effiziente Schutzstruktur zu erreichen, werden Parameter wie optische Signale, Lichtsender, Detektoren, die Schutzschicht, und die Position der Strukturen gemeinsam optimiert.

In dieser Arbeit werden zwei dafür geeignete optisch aktive Dünnschichten entworfen und im Sputterverfahren hergestellt. Die Schichten werden durch Ellipsometrie und

Automatisierter Reflexions-/Durchlässigkeitsanalysator (ARTA) charakterisiert. Das Konzept des Schutzmechanismus wird durch elektrische Messungen an der IC-Struktur bewertet. Der Fotostrom der Detektoren wird sowohl analysiert, wenn die Schicht auf der IC-Rückseite aufgebracht ist, als auch wenn die Schicht entfernt wurde. Die Ergebnisse bestätigen den Einfluss der Schicht auf den Photostrom der Detektoren. Folglich können eventuelle Schädigungen der Schicht durch elektrische Messungen an der IC-Schaltung nachgewiesen werden. In dieser Arbeit werden auch die Vor- und Nachteile des Schutzmechanismus diskutiert und Möglichkeiten der Anwendung untersucht.

Diese Untersuchungen lassen den Schluss zu, dass die Schutzstruktur, nach der Optimierung der kritischen Parameter, zu einer vollständigen Gegenmaßnahme wird. Es wäre ein sehr kostengünstiges Verfahren und in der Lage, sowohl physische als auch optische Angriffe durch die Chip- Rückseite zu verhindern. Diese Schutzstruktur kann für alle Arten von sicherheitsempfindlichen ICs mit unterschiedlicher Größe, Technologie und Dicke verwendet werden.

Publications

The results of this research work have been presented in the following publications:

- **E. Amini**, R. Muydinov, B. Szyszka, and C. Boit, Backside protection structure for security sensitive ICs. Proceedings from the 43rd International symposium for testing and failure analysis, pp.279-284, Asm, (2017).

- **E. Amini**, A. Beyreuther, N. Herfurth, A. Steigert, R. Muydinov, B. Szyszka, and C. Boit, IC security and quality improvement by protection of chip backside against hardware attacks. Microelectronics Reliability 88-90C, pp. 22-25, (2018).

- **E. Amini**, A. Beyreuther, N. Herfurth, A. Steigert, B. Szyszka, C. Boit. “Assessment of a Chip Backside Protection. Journal of Hardware and Systems Security”, 2:345–352, (2018).

- **E. Amini**, N. Herfurth, A. Beyreuther, J. Seifert and C. Boit, "Generation and Tracking of Optical Signals inside the IC to Improve Device Security and Failure Analysis," 2019 IEEE 26th International Symposium on Physical and Failure Analysis of Integrated Circuits (IPFA), Hangzhou, China, 2019, pp. 1-6. doi: 10.1109/IPFA47161.2019.8984916

- C. Boit, S. Tajik, P. Scholz, **E. Amini**, A. Beyreuther, H. Lohrke, J-P. Seifert, "From IC debug to hardware security risk: The power of backside access and optical interaction," 2016 IEEE 23rd International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), Singapore, (2016), pp. 365-369. Doi: 10.1109/IPFA.2016.7564318.

Additionally, the author has authored the following publications:

- N. Herfurth, **E. Amini**, A. Beyreuther, T. Nakamura, S. Keil and C. Boit, "EOFM for contactless parameter extraction of low k dielectric MIS structures," 2019 IEEE 26th International Symposium on Physical and Failure Analysis of

Integrated Circuits (IPFA), Hangzhou, China, 2019, pp. 1-5. doi: 10.1109/IPFA47161.2019.8984757

- N. Herfurth, A. Beyreuther, **E. Amini**, C. Boit, M. Simon-Najasek, S. Hübner, F. Altmann, R. Herfurth, C. Wu, I. De Wolf, K. Croes, "New Access to Soft Breakdown Parameters of Low-k Dielectrics Through Localisation-Based Analysis," 2019 IEEE International Reliability Physics Symposium (IRPS), Monterey, CA, USA, 2019, pp. 1-9. doi: 10.1109/IRPS.2019.8720458

- Beyreuther, N. Herfurth, **E. Amini**, T. Nakamura, G. G. Fischer, S. Keil, C. Boit, "EOFM measurements of lateral and vertical Bipolar Transistors in Silicon and SiGe:C Technologies," 2019 IEEE 26th International Symposium on Physical and Failure Analysis of Integrated Circuits (IPFA), Hangzhou, China, 2019, pp. 1-4. doi: 10.1109/IPFA47161.2019.8984762

- Beyreuther, N. Herfurth, **E. Amini**, T. Nakamura, I. De Wolf, C. Boit,: "Photon emission as a characterization tool for bipolar parasitics in FinFET technology", In: Microelectronics Reliability, Elsevier, 88–90 (2018), S.273-276

Acknowledgments

First, I would like to express my deep and sincere gratitude to my supervisor Prof. Dr. Christian Boit, for giving me the opportunity to do research and providing invaluable guidance throughout this research. He has taught me not only the methodology to carry out the research but also important lessons for being a great person. I wish to thank my second supervisor Prof. Dr. Bernd Szyszka, for introducing me to the world of thin-film technology and guiding me through this research. I would like to express my special appreciation and thanks to Prof. Dr. Jean-Pierre Siefert for his support and encouragement for about two years and for being part of my examination committee. I am extending my thanks to Prof. Dr. Roland Thewes and his group for productive discussion, test structure designing, and lab support. Many thanks to Prof. Dr. Navid Asadi Zanjani for agreeing to review this thesis.

This dissertation has been started as a part of Helmholtz Research School on Security Technologies (HRSST) and supported by this school. I would like to thank HRSST for the scholarship and supporting me during the first 3.5 years of my thesis.

I would like to say thanks to my friends and research colleagues, Anne Beyreuther and Norbert Herfurth, for their support throughout this research work, scientific discussion, and cooperation on papers, and nice conference trips. Special thanks go to Dr. Uwe Kerst for helpful ideas and suggestions regarding possible enhancements and Stefan Keil for IC designing sample preparation, bonding, packaging, and finding solutions for technical problems.

Thanks to Andreas Eckert for sample preparation and thanks to René Hartman for bonding and packaging the samples.

It was an honor to be part of the team of the Semiconductor Devices group at TU Berlin. I would like to thank: Dr. Felice Friedrich for being a very kind mentor and helping me to present my research work. Dr. Clemens Helfmeier for teaching me how to work with very tiny devices, and Dr. Tuba Kian for fruitful discussions. Marlies Mahnkopf for thinning and polishing the samples, helping with chemistry lab work and, following people for helping me during my PhD study: Dr. Philipp Scholz, Dr. Heiko Lohrke, Silvia Rabe, Claudia Petzsch, Mathias Schulz, Dr. Ivo Vogt, Orman Gref.

Furthermore, I would like to thank Alexander Steigert (HZB) for his efforts in coating Ti and TiO2 layers and characterization of the layers. I also thank colleagues at the Technology of Thin Film Devices group; Nivin Alktash and Marlene Härtel for helping me with ellipsometry measurements; Manuel Hartig and colleagues at PVcomB for coating and characterization of the thin films.

I am extremely grateful to my parents for their love, prayers, caring, and sacrifices for educating and preparing me for my future. I am very thankful to my husband, Dr. Mohammad Reza Mohammadi, and my beloved son, Arya, for their love, understanding, and continuous support. I wish to thank my friend Dr. Fatemeh Ghader,

for all her supports and helps in difficult moments and for cheering me up all the time; I appreciate your friendship, dear.

Contents

List of Abbreviations

TiO2	Titanium dioxide
Ti	Titanium
RC	R: Resistor, C: Capacitor
PVD	Physical vapor deposition
PUF	Physically Unclonable Function
PEM	Photon emission microscopy
PD	Photodetector/Photodiode
PAD	Prob attempt detector
LED	Light-emitting diode
LE	Light emitter
LAPD	Low area probing detector
ITO	Indium tin oxide
IR	Infrared
IP	Intellectual Property
IC	Integrated Circuit
FIB	Focused Ion Beam. Machin used in failure analysis
ESD	Electrostatic discharge
EL	Electroluminescence
CVD	Chemical vapor deposition
CSD	Chemical solution deposition
CPU	Central processing unit
Ag	Silver
ARTA	Automated reflectance/transmittance analyzer
AOI	Angle of incidence

Summary of the Thesis

1. Idea and Motivation

This research work aims to develop an efficient and cost-effective protection structure of ICs against hardware attacks through the chip backside.

1-1. Why is the security of the backside so important?

In recent years it has been proven that attacks from the chip backside are a significant risk for security devices. One of the reasons is that because the optical techniques on the backside are able to produce quantitatively significant signals, adversaries can drive any nodes and extract the information. Such attacks are performed through the backside not only because the backside is unprotected, but also the nodes can be easily accessed through the backside, and the precision can be increased. All countermeasures implemented on the IC frontside can be circumvented by attacks through the silicon backside. This fact reveals how the security of the backside is significant.

A review of the attacks carried out from the chip backside indicates that such assaults can be divided into two categories: the first category involves all the attacks which physically damage the IC backside, for instance, through milling the silicon substrate or making a hole using FIB and microprobing. The second category contains attacks that are carried out without any physical tampering (without chip preparation or silicon thinning), using optical techniques through the silicon backside.

1-2. What are the features of an appropriate protection structure for the chip backside?

An appropriate protection structure to shield the device against infiltration would have to detect any external interference to the chip backside and must be opaque to the infrared (IR) wavelength. IR is the wavelength of the photoemission from silicon devices; the silicon substrate, which makes up the IC backside, is transparent to the IR lasers as well. Furthermore, the protection structure should be inexpensive and should not present area overheads.

A cost-efficient way to electrically connect the backside to the frontside of an IC currently does not exist, except with through-silicon via (TSV), which is expensive. So, the backside is not easily electrically protectable. Therefore, the natural way to design a protection structure should be based on optics. In other words, it is necessary to have a structure on the chip backside as well as optics to provide a signal that is specific to this structure.

2. Introduce, develop, realize and evaluate a protection structure for the backside

2.1 Backside protection enters the new ground, and basic research is required

Designing a protection structure based on light is not an easy job, and it has many requirements. First, the optical signal must be generated inside the chip so, a light emitter inside the IC is needed. Second, the optical signal must travel through the silicon bulk; hence, the optics must be in the range of the wavelength to which silicon is transparent. The third requirement is that the optical signal should carry some information about the IC back surface. Thus, the optics must interact with the backside, and the back surface must affect the optical signal. The fourth necessity is a detector that is capable of detecting the optical signal and converting it to the measurable electrical signal by the IC. In order to have a successful protection structure, all these four parameters need to be optimized. All these critical factors influence each other and must be optimized together.

2-2. Light emitter

In order to generate the optical signal inside the semiconductor chip, it is necessary to have a light emitter that is able to emit inside the chip in a spectral range that silicon is transparent to. The only available structures within the IC are located on the circuitry side, i.e., the IC elements. Thus, an IC structure must be used as a light emitter. In each modern IC, there are plenty of transistors - devices that contain a drain, a source, and a gate. The drain and the source of the transistors are the regions where an n-type semiconductor is doped into the p-type silicon bulk (for n-type transistors). The boundary of the doped area in the silicon bulk forms a p-n junction. A forward-biased p-n junction is a light emitter device that is capable of emitting photons. As almost all available chips are made of silicon, the only option is to use a silicon p-n junction as a light emitter (LE in Fig 0. 1). Although silicon is an indirect semiconductor, electroluminescence still occurs. However, to generate sufficient photons, a high-level of voltage must be applied to a silicon p-n junction. A forward-biased silicon p-n junction creates photon energies close to the silicon bandgap (infrared region) with a deviation of around 0.1eV. The generated photons are partly absorbed by silicon bulk when traveling inside the chip. The intensity of the photon in each point inside the silicon strongly depends on the energy of the photons, traveling length, and properties of the silicon bulk. When the silicon bulk is low doped, the absorption rate in the silicon bulk is lower. To generate an optical signal inside IC, which must be transportable inside the silicon bulk and detectable by detectors, some parameters of the light source such as the size of the device and input power to the light emitter must be optimized. The generation and transportation of photons in silicon are discussed in more detail in Chapter 2.

2-3. Light detector

To observe the IC back surface optically, the optical signal that carries information about the backside must be detected and transformed into a measurable electrical signal. For this purpose, the drain and the source of transistors can be used as light detectors (PDs in Fig 0. 1). A reverse-biased p-n junction acts as a photodetector, where the absorbed photons create a current. The current is directly proportional to the intensity of the incident light. Therefore, measuring the photocurrent of detectors provides specific information about the backside.

2-4. Protection structure

As mentioned before, a proper protection structure for the IC back surface must be opaque to the IR light. This structure can be an opaque layer coated on the chip backside. Since the backside is not electrically controllable, the monitoring of the coated layer must be performed optically. Hence, the optical signal must carry some information about the protection structure. The opacity of the layer is necessary but not enough; in addition to opacity, the layer coated on the back surface must affect the optical signal. Therefore, the protection layer must be optically active and change the optical signal. Both light-emitting and light-sensing devices are placed on the circuitry side of the IC. The light emitted by the sender travels toward the IC backside, and after interacting with the back surface reflects toward the circuity side, which will be detected by the detectors. Therefore, the backside layer must change the reflection of the light. As can be seen Fig 0. 2 infrared reflectivity of the silicon-air interface versus angle (blue line) shows that for angles larger than 17°, there is a total reflection. The most interesting property that the protective layer may provide could be angle-dependent reflectivity. The optical signal generated by the light emitter after traveling through the silicon bulk reaches the backside; then, it must be affected by the protective layer. Since, in the absence of the layer, the reflectivity for the angles larger than 17° is 100%, the layer must reduce the reflectance. In order to take advantage of the angle-dependent reflectivity property, the reduction must be dependent on the angle of incidence. Accordingly, the light detectors must be located at different intervals from the light emitter to detect light with the different angles of incidence. The story is illustrated schematically in Fig 0. 1. A critical issue about the layer is that how the reduction in the reflectance should be, in order to be beneficial in this method; the reflectivity depends on the generated optical signal, the dimension of the chip, and the depth of the bulk silicon which determines light path length and location of the detectors. The light that needs to be detected in a wide angle must travel considerable lengths inside the silicon (especially when the silicon bulk is very thick), which exponentially reduces the intensity of the light. Consequently, the ratio of the noise to the signal on the detector increases. Therefore, for the layer to have a noticeable effect on the signal of the detector, it would be beneficial for the layer to provide a substantial reduction in reflectivity at large angles. On the other hand, to have a strong enough optical signal at greater distances, a higher power must be applied to the light emitter, which is unfavorable. One needs to make a trade-off between applied power to the light emitter and reduction of the light intensity made by the layer.

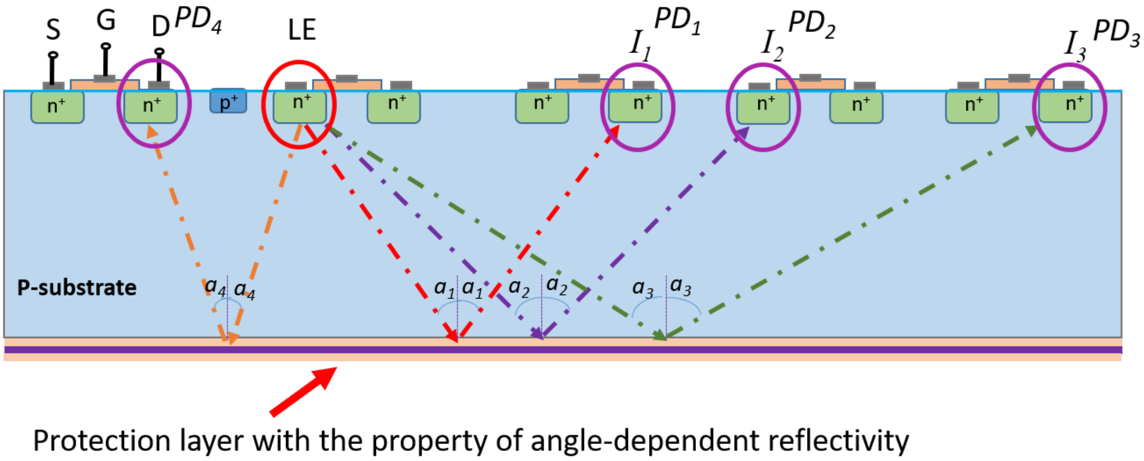


Fig 0. 1 Schematic of the protection concept: the cross-section of the IC where the IC backside is protected by a protection layer that provides angle-dependent reflectivity. The drain of a transistor (LE) is operated in forward bias condition and acts as a light emitter, emitting light in all directions inside the silicon towards the IC backside. The light reflected on the chip backside travels through silicon bulk and is absorbed by the drain of the transistors placed at different intervals from the LE operating in reverse bias mode and acting as detectors.

2-5. Design and production of the protection layer

In order to achieve a proper protection layer, several parameters need to be defined, such as which kind of material to use and which technology to use for depositing the layer. The thickness of the layer and the condition of the deposition process (e.g., temperature, pressure, power) must be optimized. There is a wide range of materials that must be tested. In this work, the reflectivity of several materials like aluminum (Al), gold (Au), titanium (Ti), and, silver (Ag) as well as their combination with the oxide layers such as TiO_2, ITO, SiO_2, are investigated by using a simulation technique. Among them, a layer of silver sandwiched between two layers of indium tin oxide (ITO-Ag-ITO) and a layer of titanium sandwiched between two layers of titanium dioxide

(TiO_2-Ti-TiO_2) can provide the angle-dependent reflectivity property and can be opaque to the infrared light. Fig 0. 2 illustrates the reflectivity of the silicon coated by the mentioned layers. The required thickness of the layer has been determined by a model. In this work, the layers are deposited on the IC backside by the magnetron sputtering at room temperature. The deposition process is optimized to achieve the layer with the needed thickness and properties defined by modeling. The deposition technique, optimization, and characterization of the layer are discussed in the third chapter.

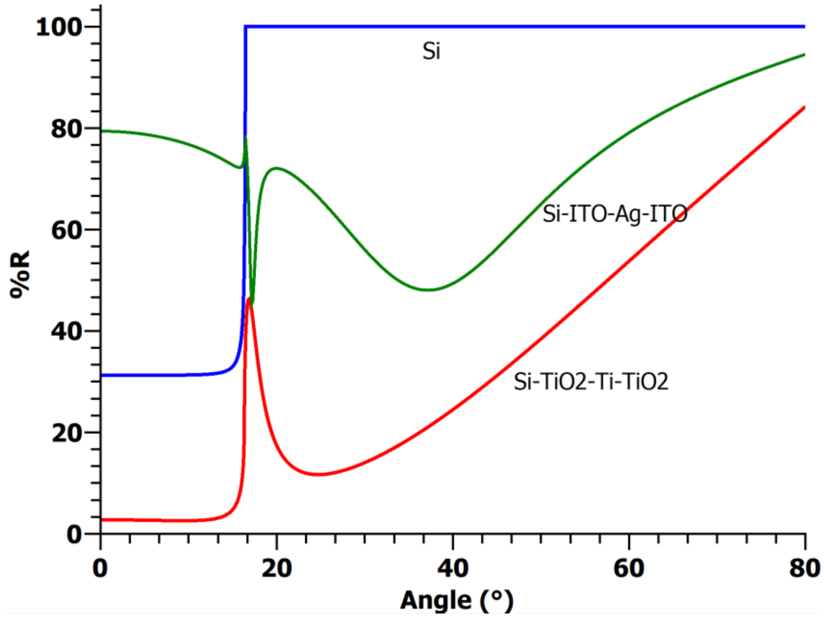


Fig 0. 2 Calculated reflectivity of silicon back surface (blue line), silicon coated with ITO-Ag-ITO (green line), and silicon coated with TiO2-Ti-TiO2 (red line) at a wavelength of 1110nm, the light source and detector are assumed inside the silicon.

2-6. Attack detection

In this protection mechanism, the integrity of the protection structure is checked by observing the signal of the detectors. For this purpose, the photocurrent of detectors is measured, while the backside is covered by the protection layer. A pattern of the ratio of these photocurrents is stored on the IC. To check the integrity of the layer, each time the same measurement on the detectors is performed and compared to this pattern. The pattern must be the ratio of the photocurrent of the detectors, but not the absolute value of the photocurrents to avoid the effect of the changes in the input voltage on the pattern. According to Fig 0. 1, the pattern can be:

$$^{I_1}/_{I_2} \ \& \ ^{I_2}/_{I_3} \& \, ^{I_1}/_{I_3} \qquad \text{E-1}$$

where “*I”* is the photocurrent of a detector after the layer is coated on the IC backside and is intact. As long as the ratio of the measured photocurrents is the same as the pattern and confirms the angle dependence of the intact coating, the integrity of the coating is verified, so no attack has occurred.

If the layer on the IC backside is somehow destroyed, the intensity of the reflected light will change. The changes in the light intensity result in changes to the photocurrent of the detectors. Consequently, the ratio of the signals of the detectors would not be the same as the pattern stored on the IC, which indicates that an assault happens, as shown in E-2. Therefore, the device should be disabled, or the sensitive data should be cleared away by disabling circuitry that may be included in the device to prevent the attackers from accessing the secret data.

$$ {I'_1}/{I'_2} \;\&\; {I'_2}/{I'_3} \;\&\; {I'_1}/{I'_3} \neq {I_1}/{I_2} \;\&\; {I_2}/{I_3} \;\&\; {I_1}/{I_3} \qquad \text{E-2} $$

2-7. Test Structure

Another factor that plays a significant role is the dimension of the chip that must be protected. In this method, at least three detectors are needed, which should be placed at different intervals from the light emitter to provide a variety of angles of detection. Considering the angle-dependent reflectivity of the layer illustrated in Fig 0. 2, it is not recommended to use detectors that detect light with an angle of incidence (AOI) below 17°, as reflectivity is constant for this range of angles. Therefore, detectors must be chosen in the distances that detect light with an AOI greater than 17°. In order to use the angle-dependent property of the layer, the detectors must detect light with different AOIs larger than 17°, i.e., the angles that provide a different reduction in the reflectance, such as 25°, 45°, and 65°. Thus, the angle dependence property of the layer is a very crucial factor because it determines the place of the detectors as well as the distance that light has to travel. When the chip is very thick, the light must travel a long distance to get to the detectors; consequently, absorption of light in silicon increases, so a higher light intensity must be provided by the light emitter. One solution to detect light with a wide angle of incidence and a short light path length is to thin the silicon bulk. Another benefit of having a thin silicon bulk is that absorption in the silicon bulk is reduced; hence, less light intensity is required. A smaller light emitter or a lower power to apply to the light emitter can be used. For instance, in an IC with a thickness of 300µm to detect light with AOIs of 25°, 45°, and 65°, detectors should be placed at a distance of 280µm, 600µm, and 1287µm respectively from the light emitter. These distances change to 47µm, 100µm, and 215µm for a chip with a thickness of 50µm. Fig 0. 3 shows this schematically. Therefore, this protection mechanism is suitable for both small devices like smartcards and large devices like FPGAs. Clearly, the size of the light emitter, location of the detectors, intensity and energy of the optical signal, properties of the protection layer, and dimension of the chip are not independent of each other and must be optimized together.

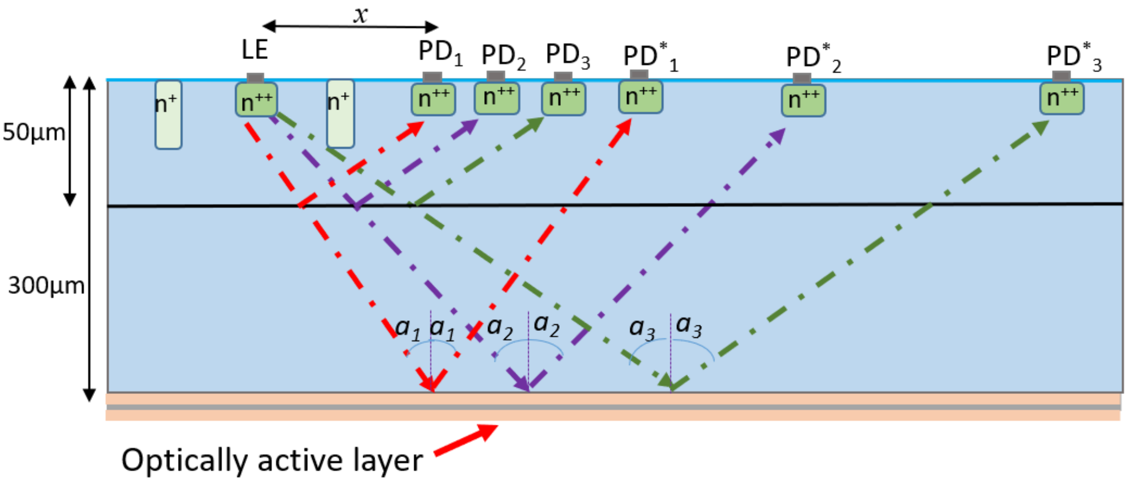


Fig 0. 3 Schematic cross-section of the location of light emitter (LE) and three detectors. The location of the detectors is determined by the properties of the layer and thickness of the chip. To detect the light with AOI of 25°, 45°, and 65°, the distance between the LE and detectors (*x*) must be 47µm, 100µm, and 215µm respectively in an IC with a thickness of 50µm (PDs) and distances 280µm, 600µm, and 1287µm when the thickness is 300µm (PDs*).

2-8. Proof of attack detection and optimizing the parameter

This work also investigates the attack detection ability of the proposed protection mechanism. The optically active layers of ITO-Ag-ITO and TiO2-Ti-TiO2 are evaluated separately. Each layer is deposited on the IC backside as the protection structure. A drain of a transistor driven in forward bias condition is utilized as a light source. The photocurrent of several reverse-biased p-n junctions is measured in the presence and absence of the layer. The effect of the layer on the photocurrents is analyzed. The photodetectors are chosen at different intervals from the light emitter, which provides detection of light at different angles of incidence. The light emitter is a high-doped silicon p-n junction, and the generated photons have energy close to the silicon bandgap (1.1 eV). Besides the fact that silicon is not an efficient light emitter as it is an indirect bandgap semiconductor, the generated photons are partly absorbed by silicon bulk before reaching the detectors. Therefore, it is necessary to apply high forward bias to the light emitter to get enough light at the farthest detector. The first issue that came up in the experiment was the degradation of the transistor, whose drain was used as a light emitter. When a high forward-bias was applied to the drain, a large number of the carriers injected into the device and damaged the gate of the transistor. To overcome this issue, an individual p-n junction is designed in the test device and utilized as the light emitter. Another issue with the light source is that when a high forward bias applied to the emitter, it may create a leakage current that travels in parallel with the light. When the light travels a long distance, this current is insignificant, but when the detector close to the light source, the current cannot be ignored. The next issue is that the light source emits in all directions; hence, some radiation can travel directly from the emitter to the detectors. This radiation has no interaction with the backside, so it does not carry any information on the backside. To prevent such problems, a structure similar to an n-well, here called guard ring (GR), is designed around the light source. This guard ring partially restricts the direct passage of light between the light-emitting and light-sensing devices and decreases the leakage current. Furthermore, the guard ring helps to keep the regular IC structure close to the light source safe from the side effects of driving a p-n junction (LE) in a high forward bias. The concept of the optimized protection mechanism is illustrated schematically in Fig 0. 4, where a single p-n junction surrounded by a guard ring is utilized as the light emitter.

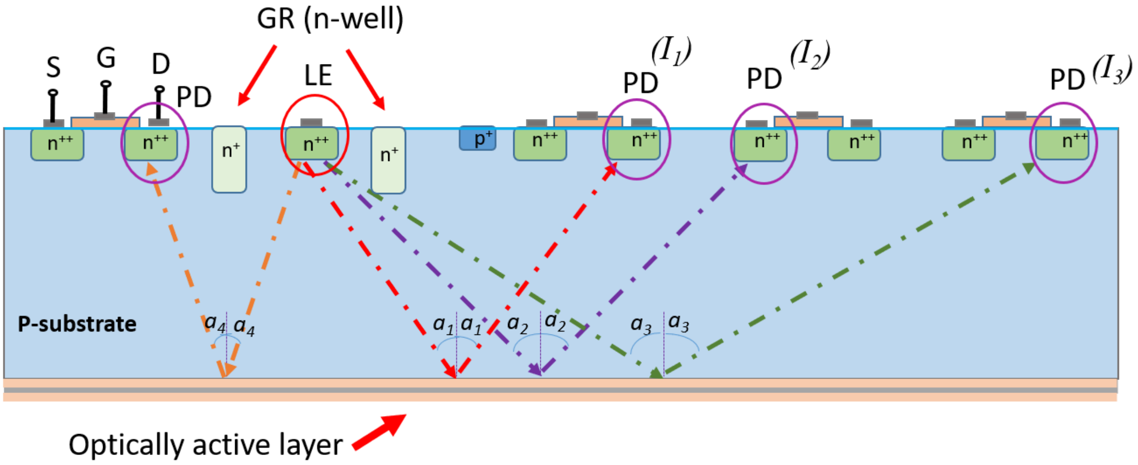


Fig 0. 4 Schematic of the protection concept: an individual p-n junction is utilized as a light emitter to generate the optical signal inside the IC, with an n-well designed around the light emitter as a guard ring. An optically active layer that is opaque to the IR light and provides angle-dependent reflectivity is deposited on the IC backside to affect the intensity of the reflected light. The drains of the transistor at different distances from the light source are chosen as the detectors, which enables light detection at a variety of angles of incidence.

After optimizing the parameters mentioned above, the attack detection ability of the protection layer is evaluated. Since this work is an exploration of a research base, and the electrical measurements are done externally via long cables to overcome the noise generated by equipment, a larger device is utilized as a prototype chip. The two devices that are used in this work are produced with 250nm BiCMOS technology. The full circuitry covers in an area of 0.5mm× 4mm in one chip and 1mm×2mm in another one. The ICs were thinned and polished to a remaining silicon thickness of 330µm and 300µm, respectively. The light emitter and detectors were the individual p-n junctions, all a size of 8µm×20µm. The protection layers were deposited via the sputtering method at room temperature on the backside of the IC. A forward-biased p-n junction surrounded by a grounded guard ring is utilized as the light emitter. The photocurrent of the detectors is measured before and after the depositions of the optical layer. Then, the layer is removed from the backside of the chip by chemical etching. The same electrical measurements are repeated. All measurements (before and after coating, and after removing the layer) are repeated three times on different days. A comparison of the value of currents proves that the measurements are repeatable and reliable.

2-9. Results

The results of the electrical measurements after all optimizations and improvements of the parameters of the method are presented in Fig 0. 5. The results indicate that the photocurrent of the detectors reduces after applying the protection layer, and the reduction depends on the AOI of light that is absorbed by the detectors. The changes in the photocurrents are in good agreement with the changes in the reflectivity of the layer coated on the silicon backside. The results confirm that the detectors absorb the reflected light from the backside and that the coated layer changes the intensity of the reflected light, affecting the photocurrent of the detectors. The results prove that the current of the detectors is not the leakage current between emitter and detector but created by the detected light from the reflections. In other words, the optically active layer coated on the chip back surface specifies the photocurrents of the detectors, and any changes to the layer (that may result from tampering) produce variations in the photocurrents and can be detected by the electrical measurements on the circuitry side of the IC.

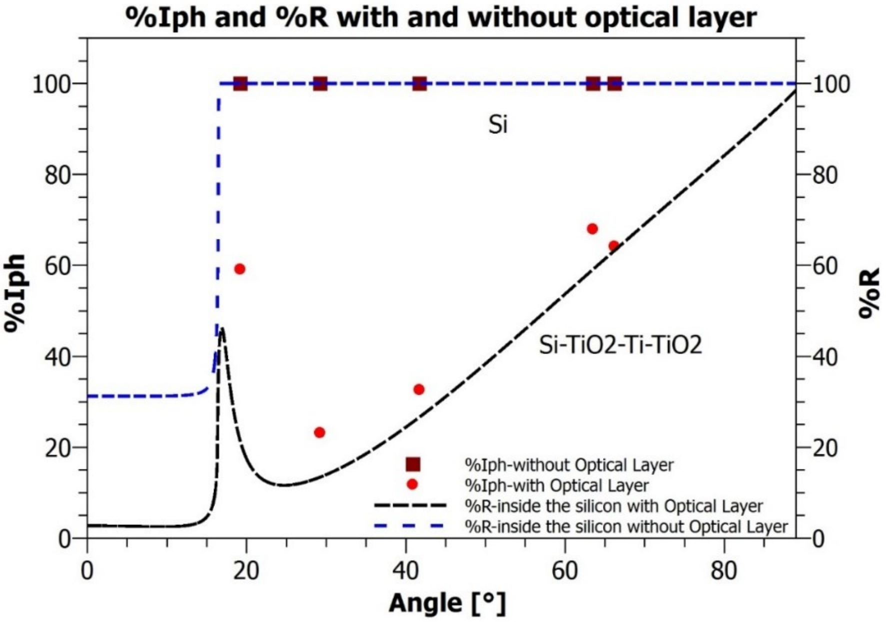


Fig 0. 5 Percentage of photocurrent of the detectors (Iph) when the chip backside coated by the optical layer (red dots), when the optical layer is removed, when the backside is exposed (brown squares), the reflectivity of the silicon (blue dashed line), and the silicon coated with TiO2-Ti- TiO2 (black dashed line)

2-10. Advantages and drawbacks

This method has many advantages. 1) It monitors the IC backside in an optical way that does not require any electrical connection between the backside and the circuitry side of the IC. 2) This method employs the electronics of the IC to signal the violation of back-surface protection. These elements are generally available on the circuitry side of the IC, even if they do not exist, making them does not require an additional step for manufacturing. 3) In consideration of contemporary technology, preparing the optical film is not expensive, and therefore, this technique is cost-effective. Furthermore, the coating process is done at room temperature, so the IC structures are not damaged by overheating. 4) There are no restrictions on the IC application and packaging since only a thin layer is deposited on the IC backside, and there is no need to encapsulate the IC. 5) There is no limitation for the silicon bulk, so the designer can utilize any thickness they want.

6) Furthermore, the signal of the detectors, which is configured by the protection structure, can be used as an identifier or a secret key to encode sensitive data. In this case, accessing the data requires a flawless protection layer. If some random roughness is created on the IC back surface before coating the layer, the reflection varies from one device to another, and the ratio of the photocurrents in each IC would be unique so that the protection mechanism would be a physical unclonable function (PUF).

Although this method has many advantages, there is a drawback as well. In most ICs, silicon is the base material. Silicon has an indirect bandgap, and consequently, the electroluminescence intensity is low. Therefore, a silicon p-n junction should be operated in a high forward bias condition to emit light sufficiently. Running the light emitter in high forward bias condition may result in the degradation of the p-n junction. It may be advantageous to assign more than one light emission spot, conduct norming measurements, and substitute the light emitter in case of device degradation. A non-silicon light source installed on the circuitry side of the IC in contact with the silicon is another alternative for generating an optical signal. The material and the characteristics of such a light source are described in the main text of this thesis. The steps of preparing the chip, the experiments, and the results of the measurements are described in detail in the fourth chapter. Furthermore, in this chapter, the advantages and drawbacks of the presented protection mechanism are discussed, and possible options to improve the method are proposed.

All in all, to achieve a proper protection mechanism, all required parameters including a light emitter, light detectors, transparency of the silicon to the optical signal, and a protection structure on the IC backside must be optimized together. In the end, when all these critical parameters are optimized together, the protection concept is attractive as it would be a very low-cost process and capable of protecting the IC against all kinds of attacks that target the IC through the chip backside.

2-11. Further research and developments

As a continuation of this work, a test structure with different sizes for transistors and p-n junctions as detectors, and an optimized light source has been designed. This test structure is produced in 180nm technology and will be used to evaluate the protection mechanism for the case that the detectors are not the same structures. In this test structure, the drain and the source of the general transistors of different sizes and single p-n junctions with different doping levels are employed as detectors.

Furthermore, a non-silicon LED has been designed and fabricated. The LED is based on GaAs that is a direct bandgap semiconductor. The LED is designed to emit light at a wavelength of 1070nm to which the silicon bulk is partly transparent to and which the IC structures can absorb. This LED will be installed on the IC frontside as an external light source. More details about the design and fabrication of the external LED are presented in Chapter 4.

An interesting development that can be made in this protection mechanism is to create random roughness on the silicon back surface before applying the protective layer. This random roughness creates a different reflection in each IC and the signal of the detectors in each device is unique. So, the protection mechanism would be a physical unclonable function (PUF). This technique is in development.

Chapter 1: Introduction

1-1 Motivation and background

Integrated circuits (ICs), also called semiconductor chips are used in a wide range of applications such as military, banking, computers, industrial internet of things (IIoT), communication devices, passports, cars, power plants, and many other devices. Nowadays, security-sensitive IC's are used not only for control purposes but to protect the confidentiality and integrity of sensitive information as well. This information may include private data, company secrets, or intellectual property (IP). Therefore, modern ICs are a popular target for adversaries to hack into.

One of the goals of hardware attacks is IP theft, for counterfeiting and overbuilding the target products. This concerns both manufacturers and end-users; manufacturers, lose their market, and end-users end up with a non-genuine product. Another motive is to get access to trade secrets to produce a competitive product or to steal the service and abuse the product [1]. In general, the aims of attacks are theft of service, cloning and overbuilding, IP piracy, and denial of service [3],[4]. The importance of the safety of the data stored on the chip indicates that adequate attention must be paid to the security of the device.

So far, many countermeasures and IC authentication techniques have been developed to protect a system from hacking and cloning in hardware attacks [5]. Most defenses focus on the security of the IC frontside, while the IC backside is wholly unprotected. Furthermore, attackers have access to many physical means that enable them to extract confidential information. Over the years, different methods for thwarting the available countermeasures and attacking the device have been presented by both manufacturers and researchers. They have shown that physical attacks can circumvent these protection mechanisms through silicon backside. This work aims to introduce and realize a protection structure to defend the IC against hardware attacks that target the chip through the IC back surface.

This chapter is designed to give the reader a brief overview of attacks on the hardware, the means needed for the assaults, and available countermeasures against such attacks. Then, a protection mechanism is presented.

1-2 Hardware security attacks, required equipment, and countermeasures

1-2-1 Hardware attacks

In general terms, hardware attacks can be grouped into three categories based on the degree of the required device modification before analysis: non-invasive attacks, invasive attacks, and semi-invasive attacks. The attacks can be either passive or active. Passive attacks are also called side-channel attacks and monitor the analog characteristics of a chip or the electromagnetic radiation from the device during regular operation [6]. Examples of such attacks include power analysis and timing attacks. If attackers play around with the signal applied to the device, such as with the supply voltage and the clock signal, the attack is active.

In the non-invasive category, device preparation is not required, and the attacked device is not physically harmed. The attackers can analyze the device by plugging it into a test circuit or by tapping the wire. The means that attackers use for such threats are standard electrical engineering tools such as a soldering/desoldering station, multimeter, oscilloscope, power supply, logic analyzer, prototyping boards, and signal generator.

The invasive attacks require direct access to the internal component like memory. They need device preparation before the attack. If the device is packaged, the packaging should be removed. Then by using focused ion beam (FIB), chemical etching or laser-cutting allow for access to the wire that is under the passive layers of the chip. Now, the device is ready for probing and modifying. Depending on the device under attack, this attack category can be more expensive compared to the non-invasive category. Attacks like micro-probing and reverse engineering are examples of invasive attacks [7]. The equipment necessary for these attacks include tools and material for decapsulating and depackaging, micro-probing stations, optical microscope, digital camera, and micro-positioners installed on a platform.

The third category of attacks is semi-invasive attacks. These attacks are harder to implement compared to the non-invasive attacks, but much less expensive equipment is needed than for invasive attacks. In the semi-invasive methods, adversaries need to gain access to the chip surface and does not require making contact with the internal lines. Therefore, the passive layer of the chip remains intact. Attacks such as disabling security fuses using ultraviolet (UV) light, laser stimulation, and optical fault injection to modify the contents of the memory or change the state of each individual transistor are grouped in the semi-invasive category [8]. Advanced imaging techniques like IR microscopy, laser scanning, and thermal imaging can also be considered semi-invasive attacks as well [9],[10]. Hardware attacks can be performed through both the frontside and backside. Due to available countermeasures on the frontside and lack of backside protection, attacks are mostly executed through IC backside.

Following are some of the attacks carried out using failure analysis tools and techniques through the IC back surface.

a) Micro-probing attacks

Microprobing attack is an invasive attack. Microprobing is performed by attaching microscopic needles onto the internal wiring or structures of an IC. This enables attackers to read out the internal confidential information or can be used for injecting fault attacks [11],[27]. Utilizing micro probing enables adversaries to capture the decrypted data directly from the data bus of the target IC's CPU core and circuit edit to set the security and configuration fuses of the device to arbitrary values. For microprobing attacks from the frontside, attackers need to remove any layer covering the signal of interest. Performing microprobing from the IC backside has the advantages that metallization and countermeasures are not employed on the backside, and chemical etching is not needed. Furthermore, the bond wiring on the frontside remains intact. Nonetheless, backside preparation and trenching through bulk silicon substrate are required. The equipment necessary for such an assault includes a microscope, probe station, tools for thinning and milling the substrate, micro-positioner, and amplifiers. In [12], the authors utilized backside microprobing for recovering data from the IC. They recovered unencrypted data from the location where the data has already been deciphered by the hardware. They also made circuit edits through chip backside by using FIB and changing the value stored within the device's configuration and security fuses. Such modifications can be utilized to disable the hardware security function and countermeasures. This kind of attack can circumvent all countermeasures employed on the IC frontside such as active meshes.

b) Optical attacks

The second group of attacks that target the IC from the backside is optical attacks. Attacks such as laser fault injection (LFI), laser stimulation, photon emission microscopy (PEM), laser voltage probing (LVP), laser voltage imaging (LVI), and electro-optical frequency mapping (EOFM) fall in this category. Executing such attacks does not require expensive laser equipment and can even be performed with a second-hand laser. The attacker should have access to the laser scanning microscope (LSM).
Optical techniques enable adversaries to set or reset any individual bit of SRAM in a microcontroller, as well as induce faults into the cryptographic system and disrupt the process's control flow. Such attacks do not require electrical contact with the metal surface, although the silicon surface must be exposed. Thus, there is no mechanical damage to the silicon. In some cases, silicon thinning, or polishing may be required.

Laser fault injection (LFI)

One way to inject a fault into the IC operation is by using laser fault injection. In this method, a laser beam with photon energy greater than the silicon bandgap energy is focused into the IC's semiconductor regions. Absorption of the photon causes electron-hole generation in the active area of the devices. The generated carriers change the internal voltages, currents, and device parameters like switching speed, which leads to the faulty behavior of the device. Accordingly, attackers can defeat the security features of the device by manipulating the device behavior [13][14].

Laser stimulation (LS)

Laser stimulation is a failure analysis technique utilized in security analysis as well. This technique employs a laser to influence the device parameters and then examines the changes in device properties, for example, by analyzing the current or voltage consumption [15]. This results in the extraction of data or secrets from the device. Unlike fault injection attacks, such attacks do not interrupt regular device operation and do not change the data. The effect of laser stimulation can be varied depending on the laser wavelength. When the photon energy is larger than semiconductor bandgap, stimulation will generate photocarriers. This is known as photoelectric laser stimulation – PLS [16][17]. Otherwise, the photon energy of the laser induces a thermal vibration in the semiconductor device. This is referred to as thermal laser stimulation-TLS [18][19].

Optical probing attacks

Optical probing techniques are mostly used to capture the light emitted by transistors during device operation. For instance, photon emission analysis allows attackers to extract the signal processed by transistors. Photon emission analysis (PEM) is purely passive observation, which makes it difficult to detect. In addition to photon emission analysis, attack scenarios that employ laser voltage probing and electro-optical frequency mapping actively illuminate the switching transistors and drive the data by observing the reflected light. Optical probing techniques can be utilized to identify the activity map of a device to reverse-engineering the circuit. As these methods provide access to the internal signals of an IC, it can be used to extract the sensitive data stored in the device. Unlike laser fault injection and laser stimulation, in optical probing attacks, information is directly extracted from the probing beam [20][90].

1-2-2 Tools and techniques

Attackers execute physical and optical assaults using failure analysis tools and techniques such as focused ion beam (FIB), laser fault injection, and photon emission microscopy (PEM). These means enable one to study the internal operation and processes running on the hardware. FIB can be used to cut the metal layer, and polysilicon interconnects as well as to apply modifications to the IC structure with submicron precision [21][22]. Chips can be thinned and polished from the rear side down to a thickness of a few micrometers. Using FIB makes it possible to create probing points inside the chip and contact the transistors through the silicon substrate or modify the IC structure [23][24]. The PEM technique is widely used in side-channel attacks to read out the state of the transistors and to extract the data. These attacks are passive and cannot be detected by the device [25],[26]. A PEM analysis can be performed either through the frontside or the backside. In modern ICs, multiple metal layers on the frontside block the light path. Therefore, observing photons through the frontside is almost impossible, and the analysis must be performed through the IC backside.

While these techniques are mostly expensive and generally only accessible in industry and academia, some old tools are available at a lower price in second-hand markets or can even be rented hourly.

1-2-3 Countermeasures

Over the past years following the emergence of the hardware attacks, a number of countermeasures have been integrated into the chip or proposed to mitigate the attacks [27]. For instance, in modern security devices, memory has been encrypted [28]. Technological developments in fabrication technology also provide effective defense mechanisms. For instance, smaller feature size and glue logic design makes reverse engineering much harder and increases the cost of the attacks. Existing multiple interconnects layers on the IC frontside obstructs the light path, making attacks through the frontside less feasible. So, the layers need to be removed before an attack can proceed.

Modern security-sensitive devices include clock frequency sensors to prevent clock glitching attacks, random clock jitter to make power analysis harder, internal voltage sensors to protect the device against power glitch attacks, and internal bus hardware encryption to make data analysis more difficult. Another countermeasure is the use of active shields, which are implemented on top of the metal layer. These shields carry digital signals which are monitored continuously to detect any harms or milling in the metal layer. If there is a disconnection or modification in the shield, the chip will not operate anymore [29]. Analog shields and sensors such as probe attempt detectors (PAD) and low area probing detectors (LAPD) use analog features like capacitance measurement or RC delay on wires to detect probing attacks [30][31].

Most mentioned defenses focus on the security of the IC frontside and are ineffective against attacks that target the IC backside. Due to the increasing number of interconnected levels and implemented countermeasures on the IC frontside, executing attacks through frontside has become significantly more complicated. On the other hand, lack of backside protection and the existence of mounting technology like flip-chip and ball grid arrays have made the IC backside more suitable for the attacks.

Although several countermeasures against attacks targeting the IC backside have been proposed by researchers, no approach has so far been applied commercially. The reasons for this include overhead from fabrication costs, area, durability and manufacturability concerns, and issues with the reliability of such countermeasures.

One countermeasure is to include ring-oscillator PUFs as sensors to detect the incident laser signal and trigger an alarm on attacks [32][33]. Another countermeasure proposed by Manich et al. is to add a backside polishing detector to monitor the thickness of the bulk silicon existing below the active regions. This countermeasure protects the ICs only against mechanical polishing [34]. The pyramid structure proposed in [35] is a pyramidized silicon layer or pyramidized metal layer between dielectrics materials on the frontside or on the bottom of the first metal layer (M1) to mitigate the optical probing attacks. This structure scatters the incident laser light, leading to incorrect information being extracted and making optical attacks practically infeasible.

In [36], an anti-tampering encapsulation for the ICs has been proposed where the IC is encapsulated with a light-transmissive material, possessing a plurality of randomly distributed property-modifying particles and covered by reflective material. This protection structure can be opaque to the IR light but restricts the application range for the IC, as the IC must be surrounded by such a structure. In 2012, Frank Zachariasse proposed a backside tamper protection for semiconductor devices [37]. He suggested equipping the chip back surface with a light-modifying structure such as lenses, large surface roughness, or reflective particle. Then the integrity of the back surface can be checked by utilizing the IC structures to emit and detect light inside the IC. This countermeasure can prevent physical attacks that damage the IC backside but is unable to block light penetration through the chip back surface.

1-3 Scientific Contribution

This work introduces, realizes, and develops a protection structure to defend the IC against all kinds of attacks on the IC backside. Attacks targeting the chip backside can be divided into two categories: the first category involves all attacks which physically harm the IC backside, such as through milling the silicon substrate or making a hole with FIB and microprobing. The second category contains attacks that are carried out without any physical tampering (without chip preparation or silicon thinning), using optical techniques through the silicon backside. Thus, an appropriate protection structure to shield the device against such infiltrations would have to detect any external interference to the chip backside and must be opaque to the infrared (IR) wavelength. IR is the wavelength of the photoemission from silicon devices, and the silicon substrate, which makes up the IC, backside is transparent to the IR lasers as well. The protection structure presented in this work is a layer opaque to the infrared light deposited on the IC backside. This layer blocks light penetration through the IC backside. In this method, the integrity of the layer must be verified. A cost-efficient way to electrically connect the backside to the frontside of an IC currently does not exist; so, an optical approach is the natural way to think of such monitoring. Therefore, the protection layer, in addition to being opaque to IR, must affect the optical signal to provide a signal that is specific to the protection structure. In this protection mechanism, regular p-n junctions are used as the light-emitting device and light-sensing devices (photodetectors). The physics of light-emitting and light detection processes by IC structures in the semiconductor material is described in Chapter 2. The light-emitting device is aligned to emit light toward the backside of the chip. The light-sensing device is aligned to detect the reflected light from the back surface toward the circuitry side. The protection layer presented in this work provides an angle-dependent reflectivity, meaning that the layer changes the intensity of the reflected light depending on the angle of incidence. Therefore, the light detected by the photodetectors is specified by the protection structure available on the chip backside. The signal of the detectors is used to check the integrity of the layer coated on the backside. As soon as the coating is removed or damaged, the signal of the photodetectors cannot verify the integrity of the protection layer, indicating a physical backside attack. Subsequently, the device can be disabled, or the sensitive data can be cleared away by disabling circuitry, which may be included in the device to prevent the attackers from accessing the secret data. The concept of this protection mechanism is explained in detail in Chapter 2.

In this work, a protection structure is designed, which provides the angle-dependent reflectivity and is opaque to the infrared light. The thicknesses, the method and the condition of the deposition of the layer on the IC back surface have been investigated and determined. In this project, two optically active layers that meet the security requirements are introduced and their application is investigated. The evaluation results are discussed in Chapter 3. In order to investigate the attack detection ability of the protection layer, the signals of the detectors are measured electrically when the layer is applied to the IC backside. Then, the protection layer is removed from the backside of the chip, and the same electrical measurements are repeated. The results of the electrical measurements show the effect of the layer on the signals of the detectors and prove the concept of the protection method. The experiments and results are presented in Chapter 4. The results demonstrate that the described concept for protecting the IC back surface is a very promising solution to make the chip secure against attacks targeting the IC through the backside. In this thesis, the protection structure, light emitter, and light detectors are optimized and evaluated to achieve a proper protection mechanism. This work also discusses the advantages and drawbacks of the protection mechanism and investigates potential solutions to develop the protection function.

The protection mechanism presented in this work is a cost-effective optically active layer deposited on the IC backside that its integrity is checked using IC electronics. This protection mechanism can be applied to all kinds of electronic devices.

1-4 Thesis Structure

The content of this work is structured as follows. The second chapter explains the principle of the protection mechanism, how to control the integrity of the layer, and how to use the device structures to generate and detect an optical signal inside the chip. Chapter 3 gives the reader an overview of thin-film technology. This chapter presents the procedure of coating thin films on the IC back surface and demonstrates the results of the characterization of the deposited layer. Chapter 4 proves the method experimentally. The results of the electrical measurement represent the effect of the protection layer on the signal of the detectors. This chapter also discusses the advantages and drawbacks of the method and introduces possibilities for further developing the protection mechanism. Finally, in Chapter 5, the thesis is concluded.

Chapter 2: Concept of the method

This chapter describes the concept of the proposed protection structure and provides the basic knowledge necessary for an understanding of the subject. This section explains how to protect the IC against optical and physical attacks targeting the IC backside and how the general IC structures may be used to create a signal upon violation of the chip back surface.

In the previous chapter, it is expressed that attacks through the chip backside are performed through tampering with the IC backside, tracking the light emitted by the IC structures (photon emission analysis), or stimulating the IC structures by laser and observe their reaction. Therefore, a proper countermeasure to protect the security-sensitive ICs against such attacks should first detect any violation and tampering with the IC backside. Thus, some information about the IC backside is required. Second, this countermeasure should prevent the passage of light through the IC backside.

The protection structure that is presented in this work is an opaque layer coated on the IC backside, as shown in Fig 2. 1. This layer is opaque to the wavelength that silicon bulk is transparent to. The layer can prevent the passage of light and makes optical attacks through the silicon backside impossible. As long as this layer exists on the IC backside, tampering with silicon surface is impossible; therefore, no attacks are possible. Thus, it is required to check the integrity of the deposited layer.

There is no low-cost method to connect the backside of the IC to the structure located on the frontside. Hence, optics are the best way to monitor the chip backside. In order to create an optical signal to indicate a violation of the IC backside, a light-emitting device and light-sensing device are required. The light emitter and an optical receiver, such as a photodetector, are closely optically coupled and make it possible to send the information between input and output without an electrical connection.

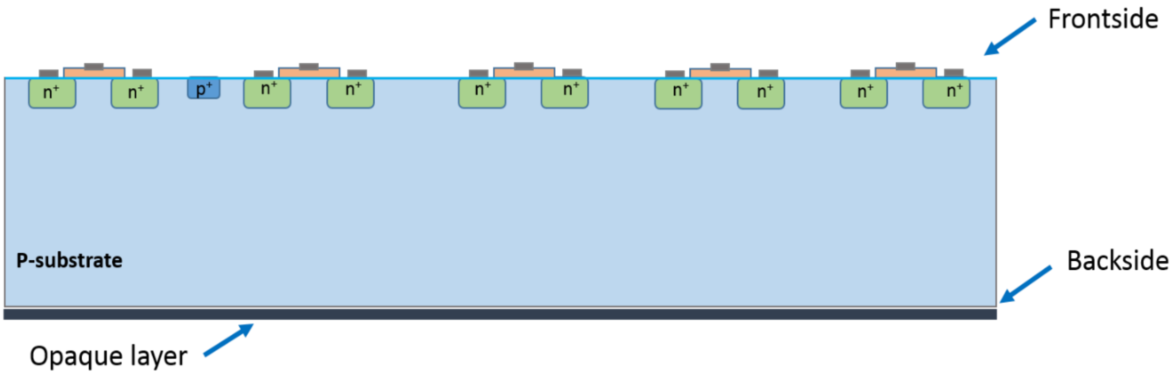


Fig 2. 1 Schematic cross-section of an IC. An opaque layer is added to the IC backside to block the passage of light through the silicon surface.

1-2 Light source and light detector

In each integrated circuit (IC), metal-oxide-semiconductor field-effect-transistors (MOSFETs) are in abundance, the device all logical and memory operation is derived from. For example, a logic gate of a modern IC is built of several MOSFETs (or FinFETs). A schematic of the memory cell is exhibited in Fig 2. 2. Each MOSFET consists of three parts, a source, drain, and gate, shown in Fig 2. 3. The source and the drain are a heavily doped region in the substrate (e.g., n-doped where the substrate is p-doped). The boundary of the doped area in the silicon bulk makes a p-n junction.

Generally, p-n junctions are fundamental building blocks of the MOSFET. Besides, p-n junctions are used in other applications, usually discrete configuration, e.g., as light-emitting diodes (LED) or photodiodes. Therefore, in each IC, there are plenty of structures that can be administered as light-emitting devices and light-sensing devices.

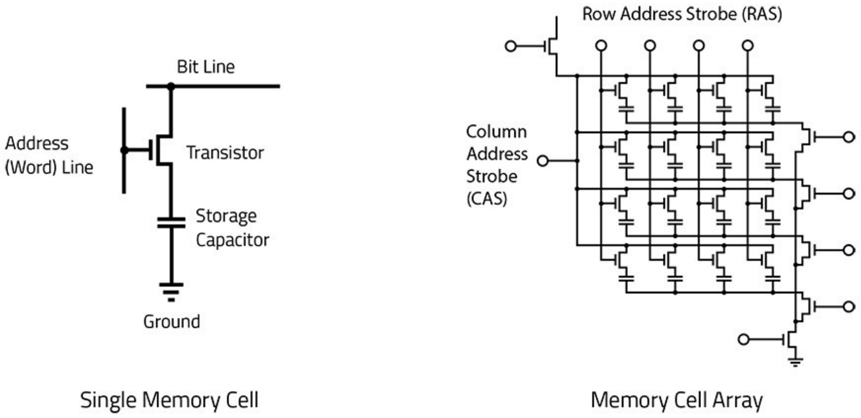


Fig 2. 2 Schematic of a single memory cell and memory cell array [38].

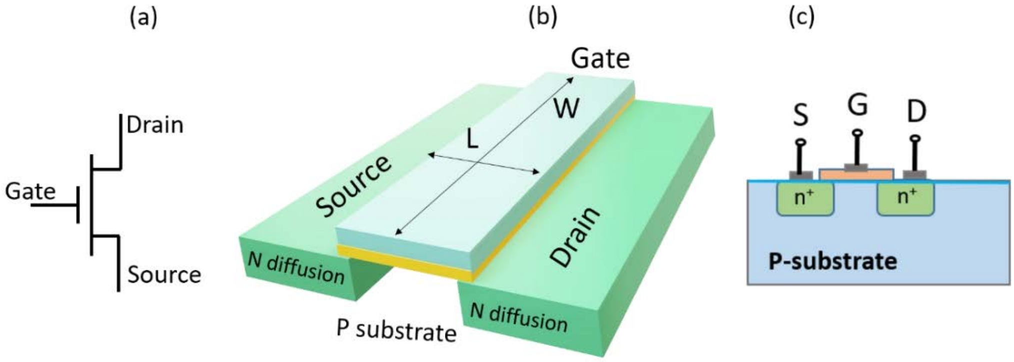


Fig 2. 3 MOS-transistor (a) symbol, (b) schematic, and (c) scheme that is used in this draft (cross-section of a transistor in a p-silicon substrate).

P-N Junction

A p-n junction is formed by joining p-doped and n-doped semiconductor materials. When a p-n junction is built in the semiconductors, electrons move from the n-side to the p-side and leave behind positive charges in the n-side. Holes move from the p-side to the n-side and leave behind negative charges in the p-side. These movements result in a current flow named diffusion current. The region where negative and positive charges are accumulated is known as the “depletion region” or “space-charge region”. The width of the depletion region highly depends on the parameters such as the type of semiconductor used to make the p-n junction and the level of doping. These positive and negative charges form an electric field directed from the positive charges to the negative charges. This electric field causes electrons to move from the p-side to the n-side and holes from the n-side to the p-side, which creates a current known as drift current. The drift current is opposite in direction to the diffusion current. Finally, there is no net current; the p-n junction comes to equilibrium, but there is a potential difference that is called barrier potential across the p-region and the n-region. These phenomena are depicted in Fig 2. 4.

By externally biasing the p-n junction with a voltage higher than the barrier potential and in the direction opposite to the barrier potential, the p-n junction would be able to conduct. This is called forward biasing a p-n junction. The width of the depletion region decreases, and the current will pass through the p-n junction. If the applied voltage is in the same direction of the barrier potential, electrons get pulled toward the n-terminal, and holes get pulled toward the p-terminal, which increases the depletion region width. This is called reverse biasing a p-n junction. In reverse bias, p-n junction does not conduct when the voltage increased. There is only a negligibly small current (saturation current) that is the result of drifting charge carriers from the junction region to the terminals.

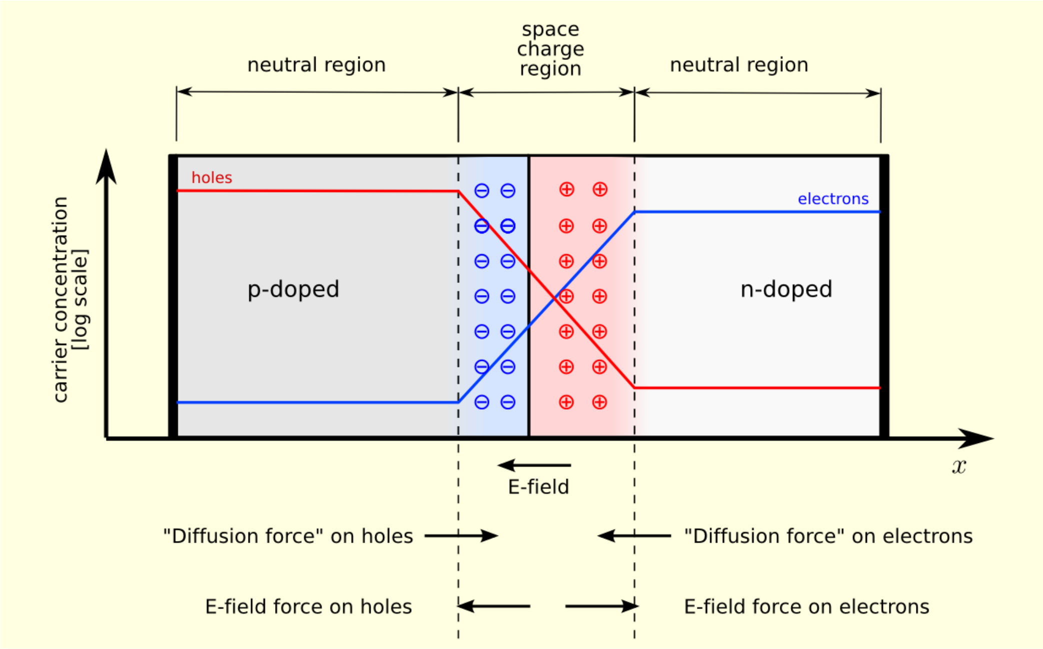

space charge region
neutral region
neutral region
carrier concentration [log scale]
holes
electrons
p-doped
n-doped
x
E-field
"Diffusion force" on holes
"Diffusion force" on electrons
E-field force on holes
E-field force on electrons

Fig 2. 4 A p-n junction in equilibrium with zero-bias voltage [39].

P-N Junction as a Light Emitter

In light-emitting diodes (LEDs), light (photon) is emitted from a semiconductor as a result of electron-hole recombination. A convenient way of achieving this is forward biasing of a p-n junction, which has the effect of injecting electrons and holes to the junction. Electrons get pulled toward the p-side, and holes get pulled toward the n-side, increasing minority carriers in the semiconductor. The resulting recombination radiation is called injection electroluminescence (EL) [40]. The intensity of the EL signal is related to the material properties such as surface recombination velocity and recombination due to defects as well as extrinsic defects during manufacturing [41][42].

The best efficiency is obtained when a direct semiconductor is used as the base material. In a direct bandgap semiconductor, the top of the valence band (VB) aligns the bottom of the conduction band (CB) in *k*-space. In an indirect bandgap material, the top of the valence band is shifted from the bottom of the conduction band in k-space and has different momentum coordinates. Band structure of the semiconductors with the direct and indirect bandgap is exhibited in Fig 2. 5. Due to this momentum gap in an indirect semiconductor, the probability of the radiative recombination is much less than non-radiative recombination [43].

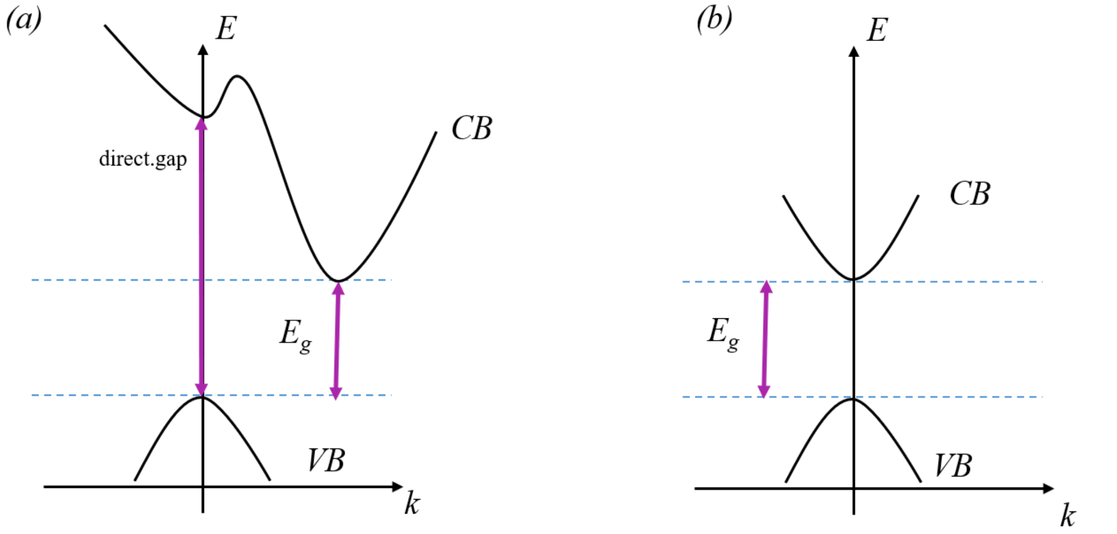


Fig 2. 5 Band structure of (a) indirect bandgap semiconductor (b) direct bandgap semiconductor. CB is the conduction band, and VB is the valence band.

A photon is characterized by either a wavelength (λ) or equivalent energy (*E*). The relationship between the wavelength and the energy of a photon is given by:

$$E(eV) = \frac{hc}{\lambda} = \frac{1.24}{\lambda(\mu m)}$$

where *h* is Planck's constant ($h=6.626\times10^{-34}$ *J.s*) and *c* is the speed of light in vacuum ($c=2.998\times10^{8}$ *m/s*), and $hc=1.24\times10^{-25}$ *J.m=1.24 eV.µm.* For instance, photons with a wavelength of 1µn (1000nm) carry an energy of 1.24eV.

As silicon is an indirect bandgap semiconductor, EL intensity is low, and p-n junctions in silicon are usually not driven as LEDs. However, the EL effect still occurs [44].

Fig 2. 6 demonstrates the integrated electroluminescence intensity of a p-n junction in silicon for several temperatures as a function of applied forward voltage. It illustrates that the LED operating condition of a p-n junction changes with temperature. Another observation can be made: the p-n junction must be driven with a high forward voltage to emit light efficiently. It can be seen that there is no EL when a p-n junction is driven at room temperature (300K) in a forward voltage below 0.6V or driven at 80K in a forward voltage below 1.2V.

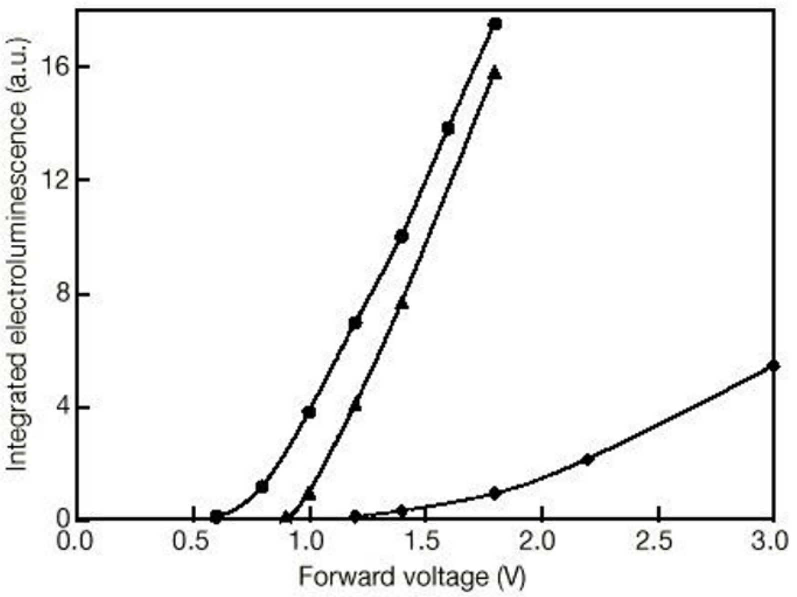


Fig 2. 6 Plots of the integral light intensity as a function of applied forward voltage at various temperatures: 80 K (diamonds), 180 K (triangles), and 300 K (circles) [45].

One parameter that affects the emission of an LED is temperature. The full electroluminescence spectra of an LED as a function of temperature (from 80K to above room temperature) are shown in Fig 2. 7 [45]. Fig 2. 7 exposes that the main peak of the EL spectra shifts to larger wavelengths for higher temperatures. At low temperatures (80 K), the main peak is at 1130nm, with a small peak at 1190, which is the phonon replica of the main peak. At room temperature (300 K), the EL spectrum peaks at 1160nm.

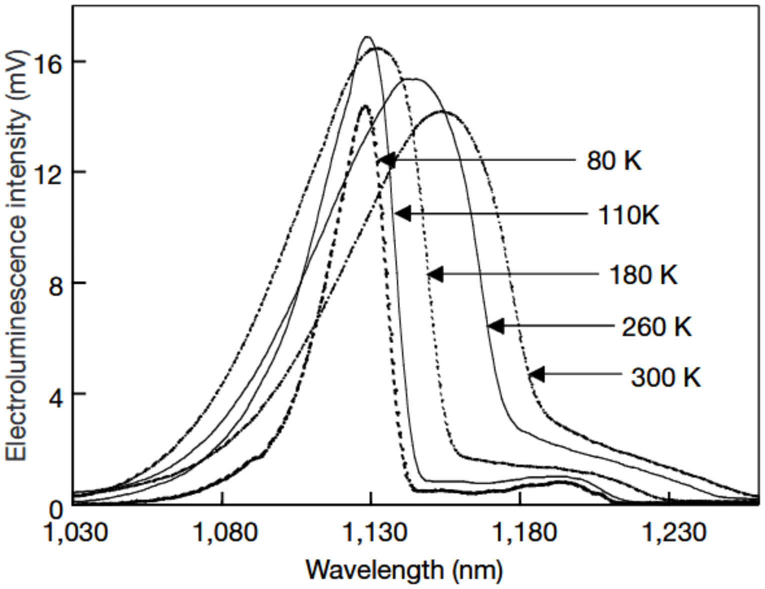


Fig 2. 7 Spectra of the electroluminescence intensity against wavelength at various temperatures[45].

Spectral and emission characteristics of a silicon photodiode depend on the bandgap energy and the doping level of the silicon forming the p-n junction. For instance, Boit in [46] has reported a spectral emission with a maximum intensity at 1110nm for silicon p-n junctions at room temperature. The spectral emission of silicon diodes extracted from the mentioned work is shown in Fig 2. 8.

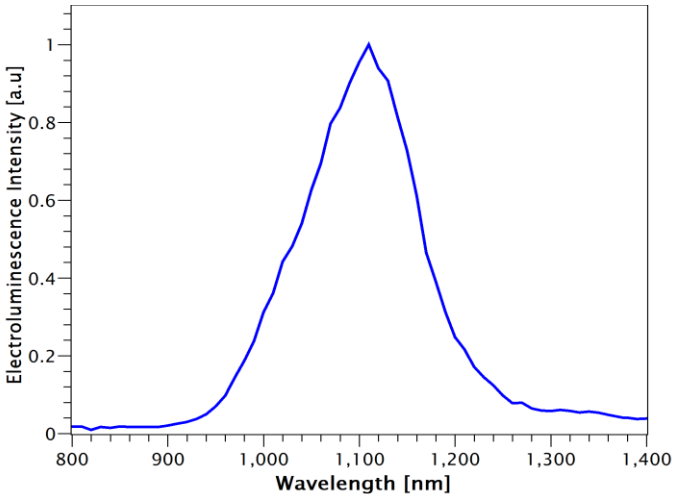


Fig 2. 8 Spectra of electroluminescence intensity of a forward-biased silicon diode at room temperature.

When light travels inside the silicon, there is a loss of energy. The loss on the energy is related to the absorption coefficient of silicon and varies for each wavelength. Therefore, the emission-spectra of Silicon LED varies at different depths in the silicon. The peak emission shifts to the larger wavelength when light travels further. The emission spectra of silicon LED at different depth in silicon is shown in Fig 2. 9.

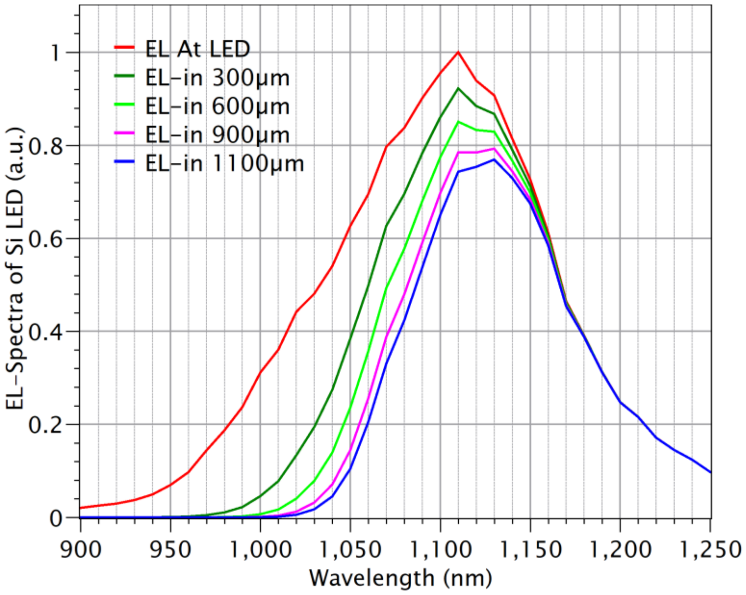


Fig 2. 9 Emission-Spectra (EL) of the Si LED at the different depths inside the silicon

In a semiconductor doped with a high dopant concentration, the broadening of the impurity band and the formation of the band-tail on the edges of the conduction band and valence band lead to a reduction in the bandgap [47]. Therefore, the imourity level is another factor that affects the emission spectrum of an LED. Falk in [48] has presented an empirical model for absorption in doped silicon. He has stated the bandgap shift caused by doping ($\Delta E(\rho)$) can be calculated with

$$\Delta E(\rho) = k_\rho \rho^{1/3}$$

where k_ρ= -1.0×10^{-8} (eV*cm) for both p and n type silicon and ρ is dopant density. Fig 2. 10 shows the magnitude of the bandgap shift versus dopant density for doped silicon. With regards to this graph bandgap shift for silicon with a doping level of 10^{17} 1/cm^3 is 4meV and reaches 46meV by increasing the doping level to 10^{20} 1/cm^3.

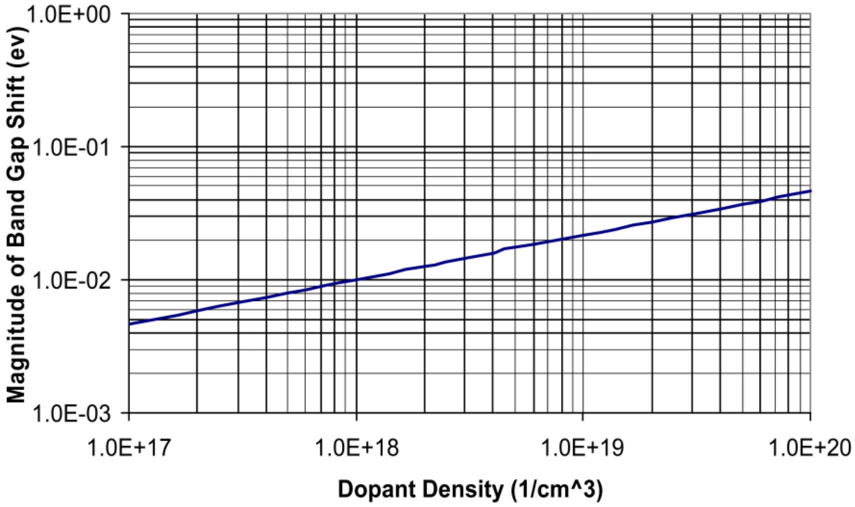


Fig 2. 10 Magnitude of the bandgap shifts versus dopant density [48].

P-N Junction as Photodetector

The photodetector is a device that absorbs light and converts the optical energy into electrical current. This process happens in two steps: 1) incident light generates electron-hole pairs, and then 2) some of the generated carriers are converted into photocurrent. Examples of photodetectors include photodiodes and phototransistors.

The critical factors in determining if a photon can be absorbed in a material are the energy of the photon and the absorption coefficient of the material related to this energy. The absorption coefficient of a material depends on the wavelength of the incident light and the carrier density of the substance. The absorption depth describes how deeply light travels in the material before being absorbed and is given by the inverse of the absorption coefficient. Absorption depth in undoped silicon is illustrated in the appendix in Fig 6. 1. Silicon with high doping level is notably absorptive in the near IR due to the bandgap shift, which affects phonon-assisted absorption and free-carrier absorption [48]. This fact has been confirmed by Fig 2. 11, which shows absorption coefficients of silicon versus photon energy and carrier density at room temperature [46]. This graph shows that doped silicon is highly absorptive in the region that undoped silicon is transparent.

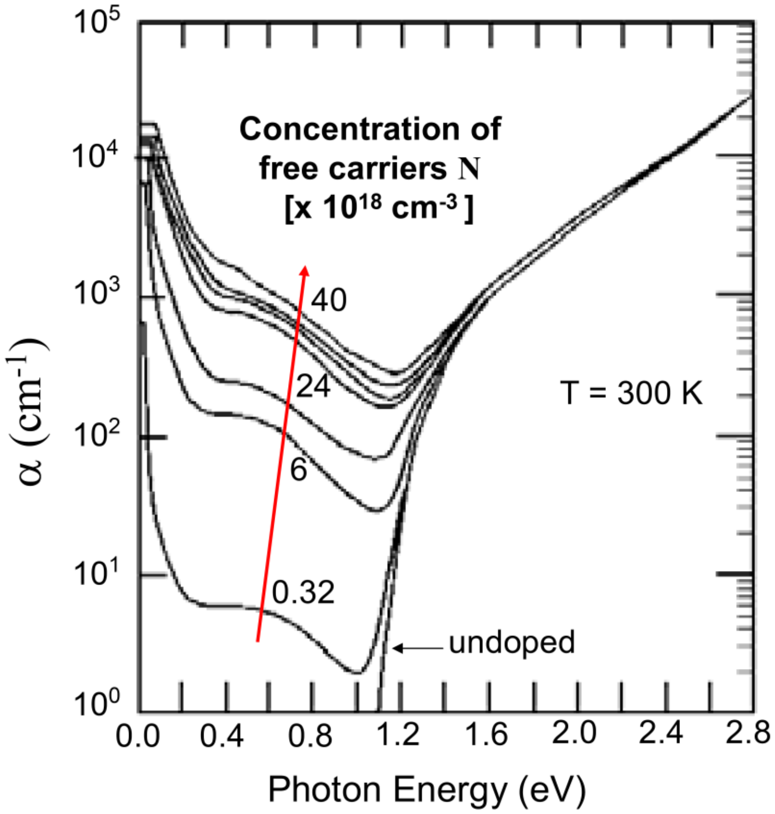


Fig 2. 11 Spectral absorption in silicon [46].

A semiconductor photodiode is a p-n junction in reverse operation. A reverse-current flows through the photodiode when the incident light falls on the photodiode. Photons absorbed in the depletion region excite electrons from the valence band to the conduction band, resulting in the creation of electron-hole pairs. The depletion region width of the p-n junction increases under reverse bias, which helps to absorb more photons. Under the effect of an electric field, these carriers move through the material and induce a current (photocurrent).

A p-n diode contains two depletion regions of the opposite type, the depletion layer width in the p-type region, x_p, and the depletion region width in the n-type region, x_n. The sum of the widths of the two depletion regions is the total depletion layer width

$$x_d\,(x_d = x_{n+}x_p).$$

From the full-depletion approximation equations of the depletion region:

$$N_d.x_n = N_a.x_p$$

, where N_a and N_d are the acceptor and donor atoms in the p-region and n-region, respectively.

$$x_n = x_d \frac{N_a}{N_a+N_d} \qquad , \qquad x_p = x_d \frac{N_d}{N_a+N_d}$$

The total depletion region width is obtained by:

$$x_d = \sqrt{\frac{2\varepsilon_s}{q}\left(\frac{1}{N_a}+\frac{1}{N_d}\right)(\emptyset_i - V_a)}$$

ε_s is the static dielectric constant of silicon, $\emptyset_i$ is the built-in voltage for the silicon p-n junction that is obtained with the equation:

$$\emptyset_i = \frac{kT}{q}\ln\left(\frac{N_d N_a}{n_i^2}\right),$$

kT/q is the thermal voltage, which is 0.026V at room temperature. n_i is the intrinsic carrier concentration, which is 10^{10} cm^{-3} for silicon.

For our device where the silicon substrate is p-doped silicon with $N_a = 5\times10^{14}$ and has an active area with $N_d = 10^{20}$:

$$\emptyset_i = 0.88 \text{ V}$$

The depletion region when 1V (in reverse operation) is applied to the p-n junction is [49]:

$$x_d = 2.22\mu m$$

For a p-n junction with a doping level of 5×10^{14} in p-side and 10^{20} in the n-side, the depletion region is almost on the p-side.

In the photodiodes, the carriers are generated either by the band to band transitions (intrinsic) or by transitions involving forbidden-gap energy levels (extrinsic), increasing conductivity. The processes of the intrinsic and extrinsic photoexcitation of carriers are shown in Fig 2. 12 [43].

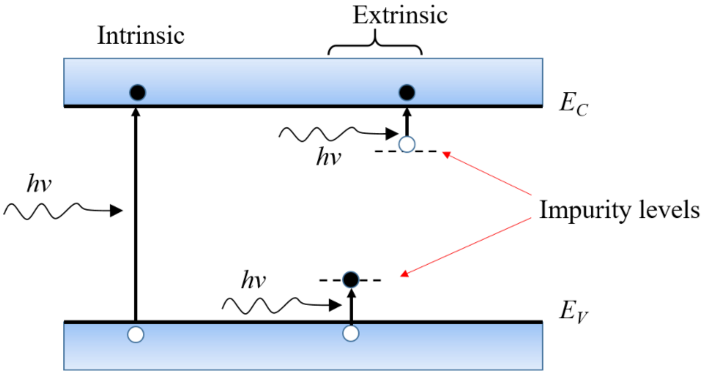


Fig 2. 12 Process of intrinsic photoexcitation from band to band, and extrinsic photoexcitation between impurity level and band.

The current-voltage relation of a p-n junction under illumination is given by

$$i = i_s\left(e^{\frac{eV}{k_B T}} - 1\right) - i_{ph},$$

with i_s and k_B as dark saturation current and Boltzmann's constant, respectively. T is the absolute temperature, V is the applied voltage, e is the absolute value of electron charge and i_{ph} is the photocurrent [40]. This relation is illustrated in Fig 2. 13, where the black line shows the dark current. Dark current is the current produced when the p-n junction is under bias but not exposed to a light source. The red line is the current under illumination, and the gap between these two lines is the photocurrent. As the dark current in reverse operation is very small, the current under illumination (red line) is considered as the photocurrent in photodiode.

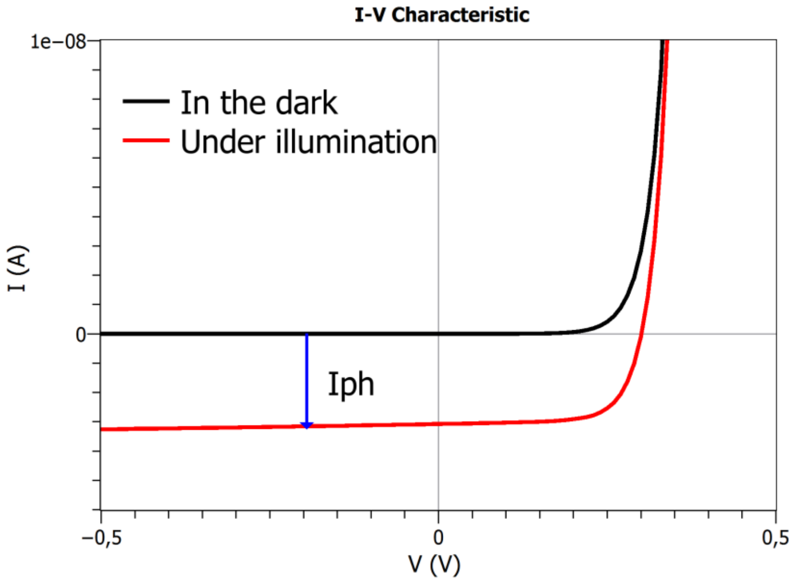


Fig 2. 13 Current-Voltage curve of a p-n junction in the dark (blue line) and under illumination (red line).

The photocurrent is directly proportional to the intensity of the incident light. The sensitivity depends on the wavelength of light [40].

In the semiconductor devices, photoelectrons are usually released from the valance band, where electrons are plentiful. Therefore, a photon needs to have an energy higher than or equal to the bandgap of the semiconductor in order to create that photocurrent.

Fig 2. 14 (black line) illustrates the spectral response of a detector (silicon p-n junction) used in this work, where the junction is placed in the depth of 310µm in the silicon substrate. This graph also shows the calculated response (photocurrent) of the detectors, where the light hits the junction after traveling 300-1100µm more in the silicon bulk. Comparing the curves explains that the wavelength of the maximum response has been shifted to a longer wavelength with the increasing depth of bulk.

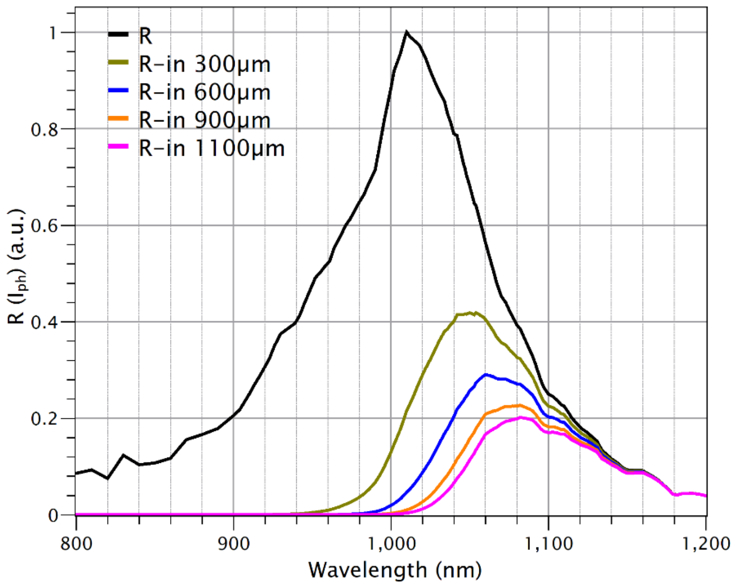


Fig 2. 14 The response of a detector (Photocurrent) over the wavelength to the light in different depths in silicon. The measured Iph (R) where the light hits the PD after traveling 310µm in silicon bulk (black line) and the calculated R for PD in the more depth of 300µm-1100µm. The light hits the detector from the IC back-surface.

Fig 2. 15 compares the spectral emission of a Si-LED and the spectral response of the photodetector. It can be seen that although the maximum emission and maximum responsivity do not occur at the same wavelength, still, there is a range of the radiation of the LED in which the detector is responsive.

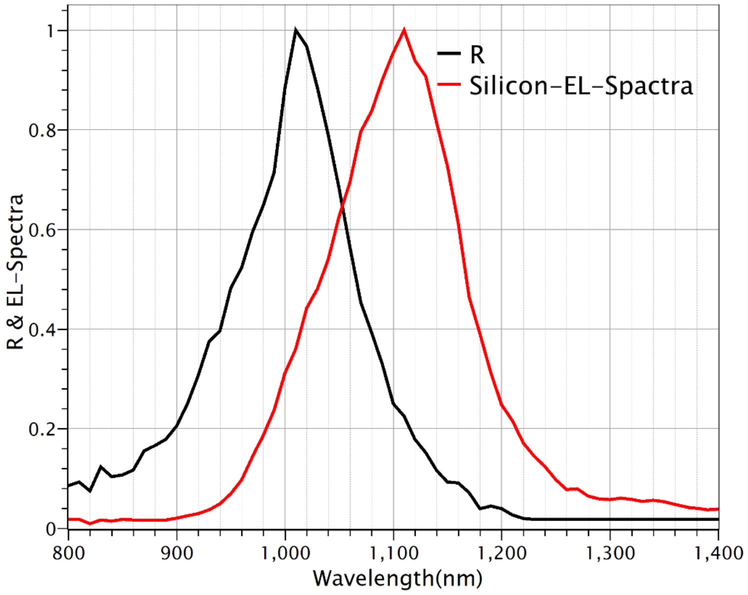


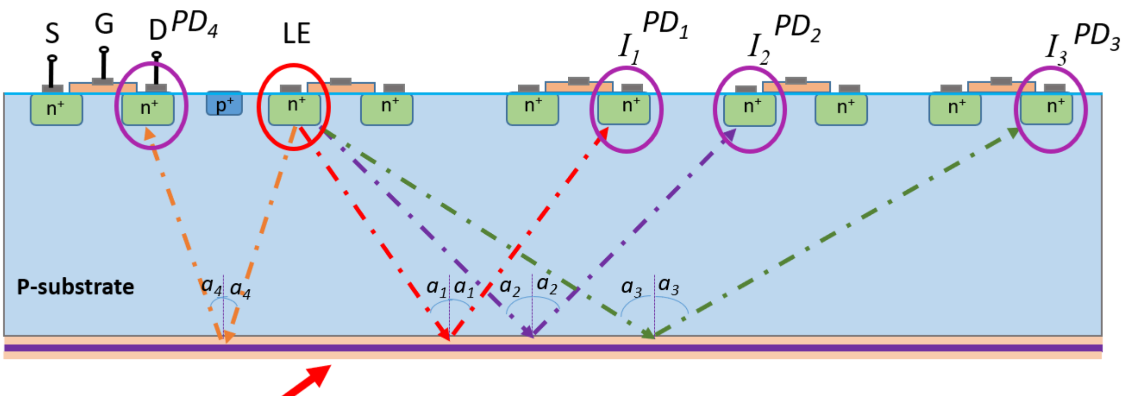
Fig 2. 15 Emission spectra of silicon LED (red line) and the response of the detector (black line).

2-2 Protection mechanism

In this method, an opaque layer is coated on the silicon back surface to protect the IC against optical attacks. The integrity of the coated layer is checked in an electro-optical way. This protection mechanism administrates a p-n junction (drain or source of the transistors) as light-emitting devices and several p-n junctions as light-sensing devices (junctions of the transistors). The light-emitting device, which is a p-n junction in the forward bias condition, is aligned to emit light toward the backside of the chip, including a wavelength range for which the substrate is transparent.

The light-sensing devices (reverse-biased p-n junctions) is aligned to detect the reflected light from the back surface toward the circuitry side. Fig 2. 16 illustrates this subject schematically, where LE stands for Light-Emitting device, and PD stands for Photo Detector (light-sensing device). A forward biased silicon p-n junction illuminates light inside the IC in all directions in the region that was discussed earlier. Some of the generated photons will be absorbed by the silicon substrate (that is, the low doped silicon), and some photons, to which the substrate is transparent, are transmitted through the silicon and reaches the back surface. The part of the photons which is reflected from the back surface will be detectable by another p-n junctions (PDs).

The intensity of the incident light on the photodetectors depends on the absorption coefficient of the silicon and light path length between the light emitter and detector.



Protection layer with the property of angle-dependent reflectivity

Fig 2. 16 Schematic cross-section of a silicon chip. Transistors are available across the IC. A p-n junction (drain of a transistor) is forward biased as a light emitter (LE), several reverse-biased p-n junctions at different intervals from LE act as light detectors. The chip back surface is covered with a protection layer.

In semiconductor devices, the drain and source of transistors are heavily doped regions. High doping densities in semiconductor cause the bandgap to shrink and the silicon to become highly absorptive in the near IR, as shown in Fig 2. 11. Therefore, detectors absorb some part of the light which has been not taken by silicon bulk.

According to the prior description, silicon is an indirect semiconductor with a bandgap of 1.12 eV at room temperature. The electroluminescence operation in silicon creates photon energies. The energy of generated photons is 5-10 % less than the silicon bandgap. Fig 2. 7 and Fig 2. 8 show the spectral emission of the silicon p-n junction (two different reports), illustrating how diodes illuminate light in infrared wavelengths with a peak at 1160nm and 1110nm respectively at room temperature.

The energy of the generated photon is sufficient to create a photocurrent in a photodiode made of highly doped silicon as well. The transport of light in silicon depends strongly on the photon energy. The physical processes responsible for photon absorption are either (a) electron-hole pair generation or (b) free carrier absorption. Both processes have to be sufficiently rare if the light is supposed to travel a long way within the silicon. The probability of process (b) is small, as long as the silicon substrate is not highly doped. The probability of process (a) in silicon is also small, as long as the photon energy is lower, equal, or only slightly higher than the bandgap. As silicon is an indirect semiconductor, in addition to photons with Si-bandgap energy, another reaction partner, a small phonon, is required. So even if the total energy is a little higher than bandgap, not many electron-hole pairs are generated. On the other hand, a considerable absorption and electron-hole pair generation at the photodetector is needed. The source/drain junctions which are used as photodetectors are usually highly doped. Therefore, the absorption rate in this region is much higher than in the low doped silicon substrate. The advantage of the 0.1 eV spectral range of the emission is that it creates enough photons with energy close enough to the bandgap in low doped silicon (low absorption for vast distance) and higher than the narrowed bandgap in the highly doped photodetector region (high absorption for strong signal).

The light emitted from the LE inside the silicon on its way to the detector must not only pass through the bulk silicon material, it also needs to be reflected on the back surface. The following section is explained what happens to a light falling on a surface.

Light reflection

Light incident on a surface will be either reflected or transmitted. Reflection (transmission) of the incident light on a surface depends on the refractive index of the two mediums and the angles of incidence of light. The index of refraction (n) for a material is the ratio of the speed of light in a vacuum (c) to the phase velocity of light in the medium (v).

n is the complex refractive index and k is called extinction coefficient

$$\underline{n} = n + ik$$

$$n = \frac{c}{v}$$

The light falling on the surface is called incident light (I), and the light reflected off the surface is called reflected light (R). The angle between the normal line and incident light is called the angle of incidence (θ_i) and between the normal line and the reflected light is called the angle of reflection (θ_r). When the surface is polished, the angle of incidence and angle of reflection are equal ($\theta_i = \theta_r$), as shown in Fig 2. 17 [91].

A ray of light which passes the surface and enters another substance with a different refractive index is called a refracted ray (T), and the angle between the refracted light and normal line is the angle of refraction (θ_t).

The amount of light reflected is determined by the reflectivity of the surface. The reflectivity can be calculated with the refractive index, angle of incidence and angle of transmission using the Fresnel equation:

The reflection for the s-polarized:

$$R_s = \left|\frac{n_1 \cos\theta_i - n_2 \cos\theta_t}{n_1 \cos\theta_i + n_2 \cos\theta_t}\right|^2$$

The reflection for the p-polarized:

$$R_p = \left|\frac{n_1 \cos\theta_t - n_2 \cos\theta_i}{n_1 \cos\theta_t + n_2 \cos\theta_i}\right|^2$$

$$R = \frac{1}{2}\left(R_s + R_p\right)$$

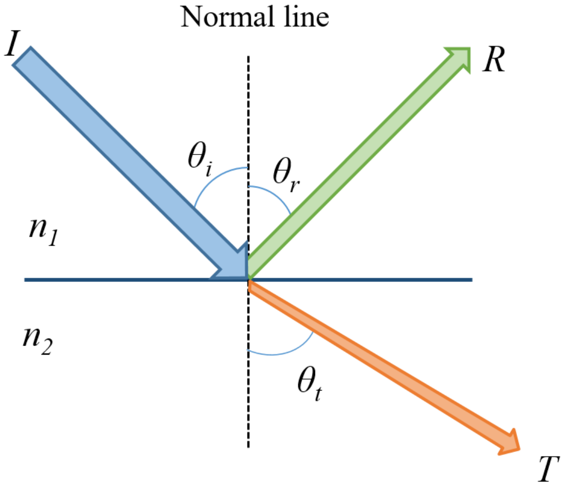


Fig 2. 17 Behavior of light at an interface. Incident (I) and reflected (R) light on the surface, refracted light (T). The angle of incidence (θi), and angle of reflection(θr), (when the surface is polished: θr= θi), angle of refraction (θt).

When the light passes from one material to another material, it slows down or speeds up, causing it to change the direction, consequently traveling at different angles. Snell's law describes how light passes through two different materials:

$$n_1 \sin\theta_i = n_2 \sin\theta_t$$

where $n_1$is the refractive index of the first material, θ_i is the angle of incidence, n_2 is the refractive index of the second material, and θ_t is the angle of refraction. The angle of incidence for which the angle of refraction is 90° is called the critical angle. For the angles larger than the critical angle, the light totally reflects off the surface, and there is a full reflection. Using Snell's law, one can calculate this angle for the silicon-air interface for light in the IR region. The silicon refractive index at a wavelength of 1110nm is 3.54, so

$$sin\,\theta_i = (n_2/n_1)\,sin\,\theta_t;$$

$$\theta_t = 90°\,,\; n_1 = 3{,}54 \;\; and \;\; n_{2(air)} = 1$$

$$\theta_i = 16.4°$$

A look at the reflectance of silicon over the angle of incidence for IR wavelengths explains how light behaves when it reaches the silicon-air interface inside the silicon. Fig 2. 18 illustrates the calculated reflectance of the silicon-air interface over the angle. For angles of incidence (AOI) larger than 16° (critical angle for silicon-air interface), silicon reflects 100% of the incident light. Therefore, the intensity of the reflected light at the silicon back surface is not related to the AOI if the angle is larger than 16°. The light source and the detector are assumed to be located inside the silicon. The curve presented in Fig 2. 18 has been simulated with SENTECH software [50].

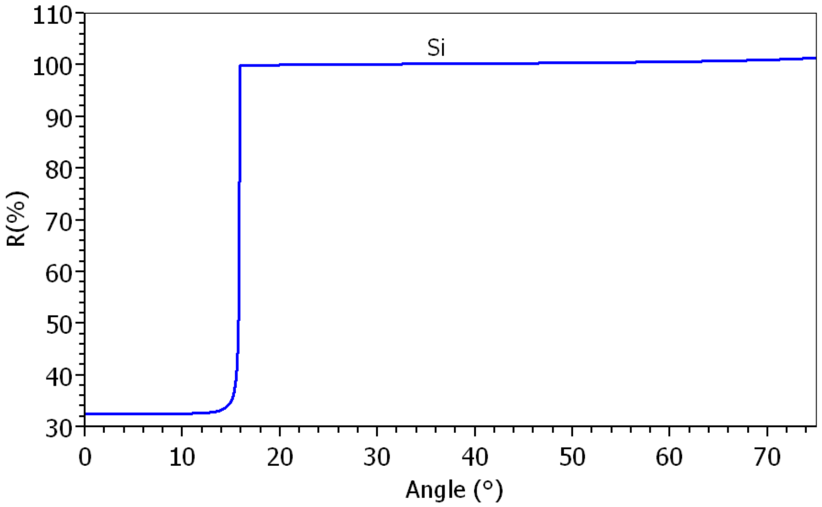


Fig 2. 18 Reflectance of the silicon-air interface various angles at the wavelength of 1110nm. The curve is calculated by the Sentech software, assuming the light source and the detector are located inside the silicon, on opposite the surfaces.

Through coating an opaque layer (protection layer) on the silicon back surface it is possible to modify the intensity of the reflected light, for instance, by coating a thin film of silver (Ag) sandwiched between two layers of Indium tin oxide (ITO), which provides angle-dependent reflection in combination with full transmission blocking. As shown in

Fig 2. 19, this layer modifies the reflectance and changes the intensity of the reflected light, depending on the AOI.

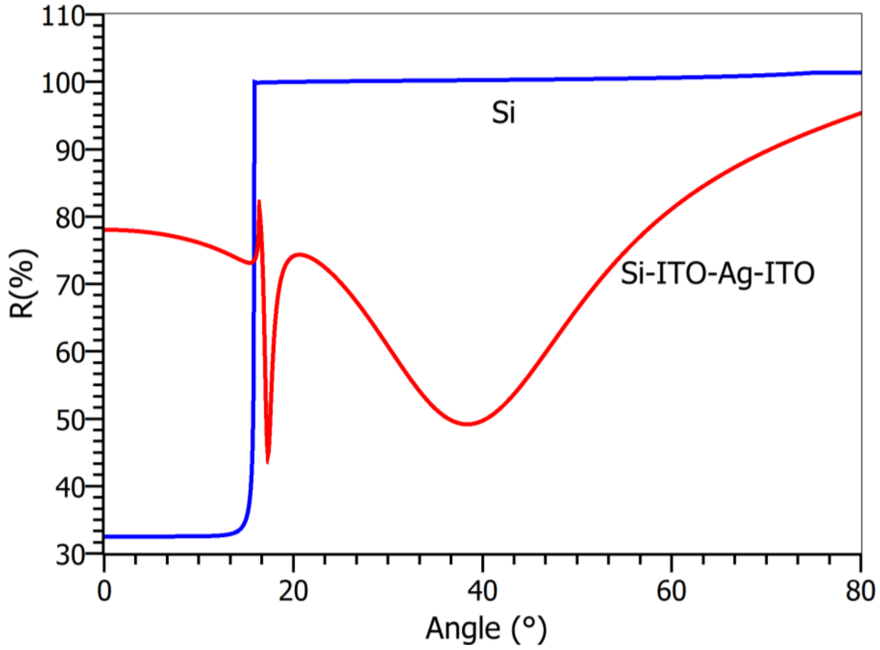


Fig 2. 19 Reflectance of the silicon (blue line) and silicon coated by ITO-Ag-ITO (red line) over varying angles at the wavelength of 1110nm. The curve is calculated by the Sentech software, assuming the light source and the detector are located inside the silicon, on opposite surfaces.

The reflected light from the silicon backside goes through silicon bulk and is then absorbed by the detectors located on the circuitry side of the IC and creates a photocurrent. Therefore, the light detected by the detectors is specified by the protection structure available on the chip backside. Then, the photocurrent can be used as a signal to indicate the integrity of the backside protection layer.

2-3 Attack detection

For attack detection, the integrity of the back-surface coating is checked by several p-n junctions used as photodetectors (PD). After coating the layer on the chip backside, a pattern of the ratio of the photocurrent of the detectors (signals of the detectors) is measured and stored on the IC. It is shown schematically in the Fig 2. 20. It is necessary to select detectors at different intervals from the LED to have a variety of reflection angles. For example, for a chip with a thickness of 50 µm to have the angles of incidence of 25°, 45°, and 65°, detectors should be located in the distances of 47µm, 100µm, and 215µm respectively from the LE. These distances change to 280µm, 600µm, and 1287µm for a chip with a thickness of 300µm.

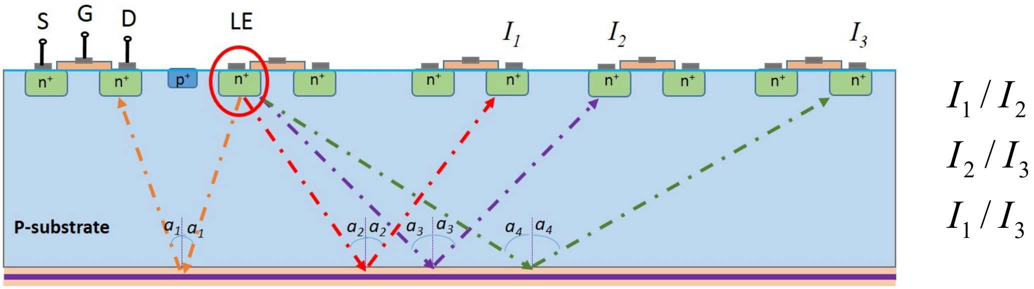


Fig 2. 20 Schematic cross-section of a chip protected by an optically active layer. The photocurrent of detectors, as well as the ratio of the photocurrents, is specific to the layer.

As long as the ratio of the measured photocurrents is the same as the pattern and confirms the angle dependence of the intact coating, the integrity of the coating has been verified, and no attack has occurred. Because the layer covers the IC backside and is opaque to the IR light, if attackers want to physically or optically assault the chip through backside (such as with FIB attacks or laser stimulation attacks), they need to damage or remove the coated layer. Since this optical layer modifies the intensity of the reflected light, removing the layer will change the intensity of the detected light as well as the photocurrent. Then the photocurrent ratio of the detectors will not be identical to the pattern. Therefore, as soon as the specific angle dependence of the coating cannot be reproduced, harm has been done to the coating, indicating a backside attack (Fig 2. 21). The device should be disabled, or the sensitive data should be cleared away by disabling circuitry which may be included in the device to prevent the attackers from accessing sensitive data.

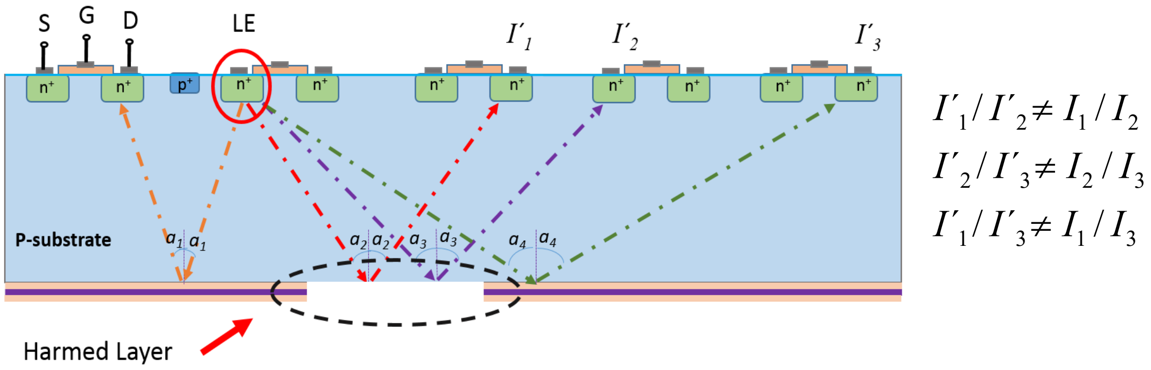


Fig 2. 21 Schematic Cross section of the chip with a harmed layer and attack detection technique.

In the method presented here, one forward biased p-n junction (forward current) is used as a light source (LE), and several p-n junctions operating in reverse bias are used as photodiodes (PD). The LE current must be limited to a safe value. If the LE is operated in a circuit with a constant voltage, it is needed to use a series resistor to control the forward current through the LE.

Monitoring the backside is achieved by measuring the signal of the detectors. P-n junctions are already available in the IC, and no additional steps in manufacturing are needed. The only extra work to have a secure IC is to coat an optically active film on the IC backside. In this case, attack detection is performed by electrical measurement on the circuitry side and accessing the chip back surface is not required.

In the following chapters, the concept of the protection mechanism is proved by coating two different optically active layer on the chip backside and analyzing the signal of the detectors in the presence and absence of the layer.

Chapter 3: Thin-film preparation

This chapter is dedicated to an overview of the production of the thin films. The methods of preparation and characterization of the layers are reviewed. The deposition process of two different optically active layers used in the defense mechanism are described, and the results of the characterization are presented. The first layer is a thin film of silver (Ag) sandwiched between two layers of the Indium tin oxide (ITO-Ag-ITO), and the second layer is a thin film of titanium (Ti) between two layers of Titanium dioxide (TiO_2-Ti-TiO_2). Both layers are capable of affecting the intensity of the infrared light reflected from the coated surface.

3-1 Thin films: Technology and Applications

Thin film is a layer of material with a thickness of less than a nanometer to several micrometers. They are very important as a means of altering the properties of the surfaces and interfaces, for example, increasing or decreasing transmittance or reflection in a certain wavelength. The features of the thin films are quite different from the bulk materials which they are made of. These properties depend on a number of the interrelated parameters, and also on the technique employed for their fabrication. The parameters that determine the optical and mechanical properties of a thin film include the thickness of the film, purity of the used target, the temperature of the process, rate of the evaporation or sputtering, degree of the vacuum inside the coating chamber, and the partial pressure of the reactive gases in the chamber.

Thin films are ubiquitous in our daily life from information and telecommunication terminals to solar cells and windows. There is a wide range of application for thin films, for instance, decoration, reflective coating, anti-reflective coating on lenses or solar cells, self-cleaning glass, and protection against corrosion and oxidation. The importance of the thin film in the semiconductor industry and the electronic is evident. The usages of thin-films in this arena are as insulators, conducting films, electrostatic coating, sensors, displays, and for metal-oxide-semiconductor field-effect transistor (MOSFET) technology in integrated circuits (ICs). Other applications of the thin films are in the memory devices as the antiferromagnetic and ferromagnetic films [51].

Insulator-Metal-Insulator (IMI) films have been widely applied to prevent surfaces from unwanted attack and to hinder the copying of products [55]. This work presents a new application of them in the hardware security of the semiconductor devices. An optical coating that consists of one or more thin films of material deposited on the IC back surface, which alters the reflection and transmission of the light on the surface. The purpose of using this thin film is to modify the reflection of light and make the surface opaque to the infrared light in order to protect the IC against attacks targeted the IC chip backside. The utilized phrases in this document, such as "optical layer," "optically active layer," and "protection layer," all refer to this optical coating.

3-1-1 Thin-film deposition method

Thin film deposition is the act of applying a thin film onto a surface. Thin films can be deposited by a variety of processes, either chemical or physical deposition techniques, such as chemical solution deposition (CSD), chemical vapor deposition (CVD), physical vapor deposition (PVD). CSD is a wet-chemical process that presents deposition methods such as sol-gel, metal-organic deposition, spin coating, and dip coating. Since this method is no vacuum technology, it has the advantages of low investment costs and low power consumption [56][57]. CVD is a vacuum deposition process in which the films of the materials are deposited from the vapor by a chemical reaction occurring on or in the vicinity of a normally heated substrate surface [58][59]. PVD is a purely physical process in which the material goes from a condensed phase to a vapor phase back to a thin film condensed phase. This method is a vacuum process and includes techniques such as sputtering and evaporation [60][61].

In this work, the magnetron sputtering technique is used to coat the optical layer on the IC back surface. The following section explains the sputtering process in more detail.

Magnetron Sputtering technique

Sputter deposition is a physical vapor deposition (PVD) method for depositing thin films. In this method, atoms are ejected from a solid target material due to bombardment of the target by energetic particles from the plasma. These ejected materials are deposited onto a substrate in a vacuum chamber and create the film [62][63].

In this process, the coating material is placed at the cathode in a solid form called target. For highly pure coating, a clean environment is needed, so the chamber must be evacuated. Then the chamber is filled with the process gas. The sputter gas is often an inert gas such as argon (Ar). However, this gas is selected based on the material to be coated and can also be oxygen or nitrogen. When a chamber is ready for the process, a negative potential is applied to the cathode, and the chamber is grounded. This electrical potential leads to creating positively charged ions of the process gas atoms. These ions are accelerated toward the target surface. The ions have enough energy to sputter some of the target material. The energy of incident ions covers the range between a few eV up to several 100 eV. The sputtered material will then be accumulated on the substrate and create a film. The process continues at a constant substrate speed until the desired thickness is achieved. The process is shown schematically in Fig 3. 1 [64][65].

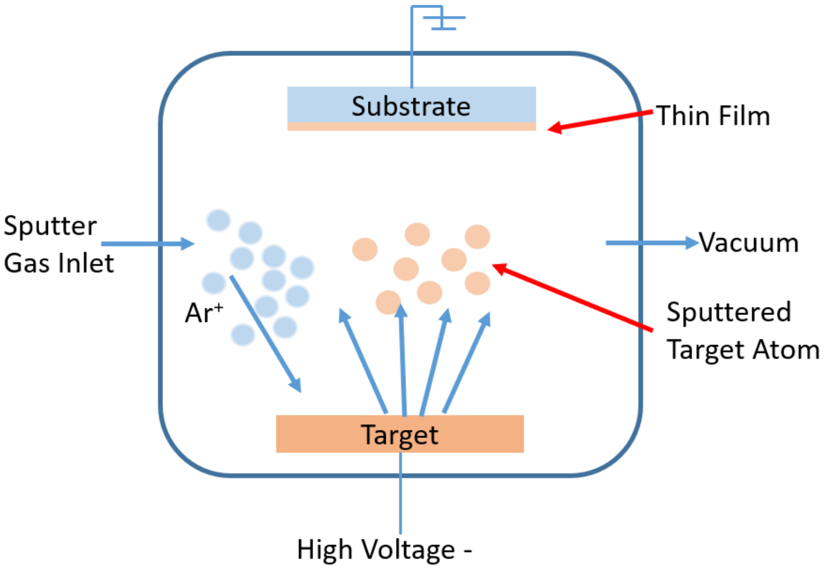


Fig 3. 1 Schematic of the sputtering process

Reactive sputtering is a process where a non-inert gas such as oxygen or nitrogen is used in the deposition process. This gas can react chemically with the target material and produces a molecular compound, which then becomes the deposited film. For example, a titanium (Ti) target reactively sputtered with oxygen (O_2) gas can produce a titanium dioxide (TiO_2) film[66].

There are several types of power supplies for magnetron sputtering. These include DC (direct current), RF (radio frequency), pulsed DC, MF (mid-frequency), and HIPIMS (High power impulse magnetron sputtering). In this work, DC and RF magnetron sputtering systems are utilized to deposit the thin films on the substrate. DC sputtering uses a DC voltage source in the kV range and is mainly used when depositing conductive materials. RF sputtering utilizes an RF power supply at a specific frequency of 13.56 MHZ. RF sputtering can be used for both conductive and non-conductive materials. Since it is more expensive than DC magnetron sputtering; its usage is mostly restricted to non-conductive materials [67].

There are several ways to characterize a thin film. In this research work, the optical properties of the films and their thicknesses are characterized using Ellipsometry spectroscopy, ARTA (Automated Reflectance/Transmittance Analyzer), and SEM (scanning electron microscopy). In the next section, the ellipsometry and ARTA spectroscopies are explained.

3-1-2 Spectroscopic Ellipsometry

Spectroscopic Ellipsometry is an optical measurement technique to evaluate the optical properties of thin films. Using optical techniques involves no physical contact with the surface and does not destruct the surface. Ellipsometry is a powerful tool used for the characterization of thin films and multi-layer semiconductor structures. In this spectroscopy, optical coefficients are characterized by evaluating the polarized light. Polarization separates light into a parallel and perpendicular component (p and s). The light beam is reflected off the sample and then analyzed to see how the sample has interacted with the light beam [68][69].

Reflection coefficients for s-polarized light and p-polarized light differ in phase and amplitude. Ellipsometry measures the complex reflection ratio ρ :

$$\rho = \tan\psi \exp(i\Delta) = \frac{r_p}{r_s}$$

where r_p and r_s are reflection coefficients of p- and s-polarized light, respectively. ψ (Psi) is related to the amplitude ratio of the reflection coefficients ψ (Psi) is related to the amplitude ratio of the reflection coefficients (ranges from 0° to 90°) and Δ (Delta) is the phase difference between them (ranges from zero to 360° or -180° to +180°). Ψ and Δ change according to the properties of the layer. When measuring a highly absorbing sample, like metals, the conventional refractive index (n) is relatively low, and the extinction coefficient (k) is large. Therefore, reflection coefficients are similar for the light of different polarization. Ψ does not change much in this case but Δ varies significantly. In low or non-absorbing materials, Ψ changes due to significant reflection [70].

Spectroscopic ellipsometry is applied to determine the optical constants and the thickness of the deposited layer on the silicon. Ellipsometers measure Δ and ψ , the quantities such as thickness and index of refraction are calculated by a model [73]. The Sentech SE 850 ellipsometer is utilized for the experiments, and the obtained data are fitted with a model using a software SpectraRay3 provided by Sentech [74]. Fig 3. 2 shows the device and the schematic setup of the ellipsometry experiment.

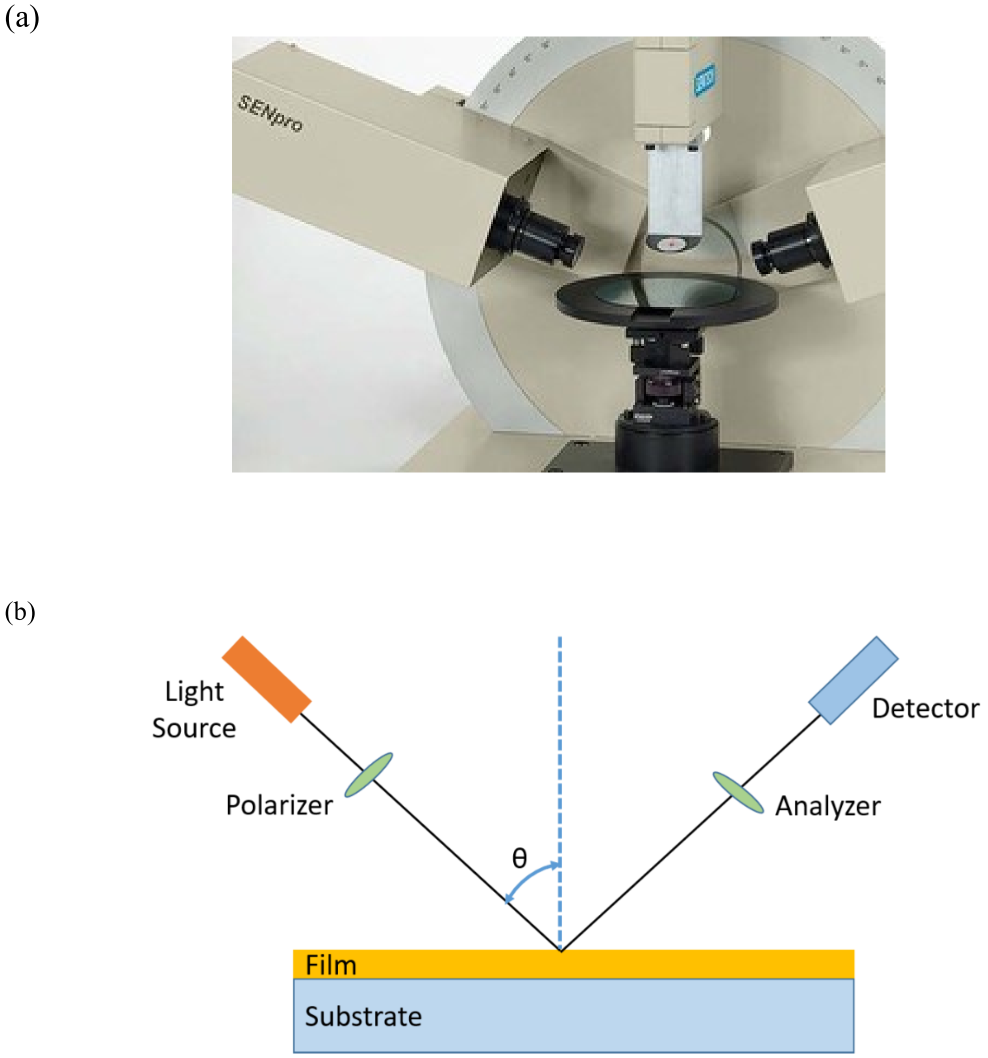


Fig 3. 2 (a) Spectroscopic Ellipsometer [75] and (b) schematic setup of the ellipsometry experiment.

3-1-3 ARTA Spectroscopy

ARTA (Automated Reflectance/Transmittance Analyzer) is a stepper motor driven goniometer tool that uses an integrating sphere as the detector in UV/VIS/NIR spectrophotometers. The ARTA is used to measure the reflectance and transmittance of the thin films over the wavelength in a range of angles. The usual range of the analyzer is 250-2500nm (limited by the range of the fiber bundle and polarizer) [76].

A sample holder is located in the middle of the sphere. The device uses a goniometer to rotate the sample, thereby varies the angle of incidence (AOI) and independently also rotates an integrating–sphere detector varying the angle of detection. Angles of incidence 0-85 degrees in transmittance and 5-85 degrees in reflectance are measurable. For any pairing of incidence angle and detection angle, spectra can be collected for s- and p-polarized light in the wavelength range of 250-2500nm. In this work, ARTA spectroscopy has been performed on Perkin Elmer Lambda 950 [77]. The ARTA device and the sample holder are shown in Fig 3. 3.

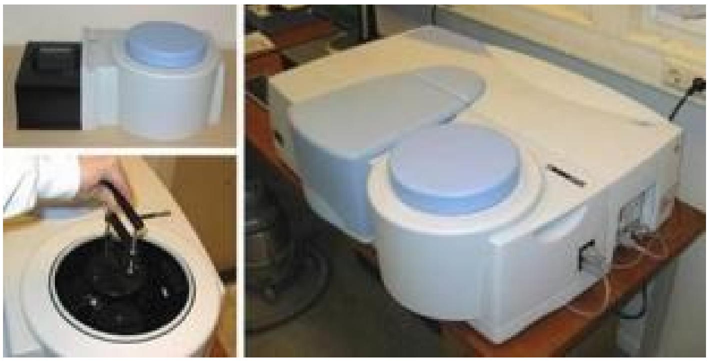


Fig 3. 3 UV/VIS/NIR spectrometer with ARTA [78].

In the following sections, the deposition process of the thin films is represented, and the results of the characterization of the two layers that are used as the protection layer in this work are shown.

3-2 Deposition and characterization of ITO-Ag-ITO

At first, to protect the IC, planar films consisting of ITO (40nm) / Ag (15nm) / ITO (40nm) are deposited on the IC backside to take advantage of the angle-dependent reflection property of these films.

The Ag IMI stacks have been deposited on the IC back surface by in-line magnetron sputtering using a Leybold Optics A600V7 vertical in-line sputter system. ITO has been deposited as an oxide film utilizing planar ceramic target DC magnetron deposition in Ar (Argon) / O_2 (Oxygen) atmosphere (2% O_2 and 98% Ar). Ag has also been deposited by planar target DC magnetron sputtering in the same machine in the Ar atmosphere. Both deposition processes were done at room temperature. Details on the process optimization of such layers are published in [79].

The coated layer is characterized by ellipsometry and ARTA spectroscopy. Spectroscopic ellipsometry is applied to determine the thickness of the coated layer. Psi and Delta are measured at two angles of incidence for light source and detector. In ellipsometry, the position of the peak along the wavelength axis is related to the thickness of the film, and the location of the peaks is related to the optical properties (index refraction and the absorption) of the film. The thickness and optical constants are extracted through a model-based analysis, using Spectraray 3 software. ITO and Ag are simulated by means of the Drude-Lorentz models. The results based on data obtained from the ellipsometer are represented in Table 3-1, and the schematic of the layer with the thicknesses is shown in Fig 3. 4. The thicknesses of the layers have been calculated using optical coefficients n and k at the wavelength of 1110nm from the Sentech database.

The fitted and measured ellipsometric Δ and ψ values are demonstrated in Fig 3. 5; the goodness of the fit is 98.1% (Mean square error = 1.9).

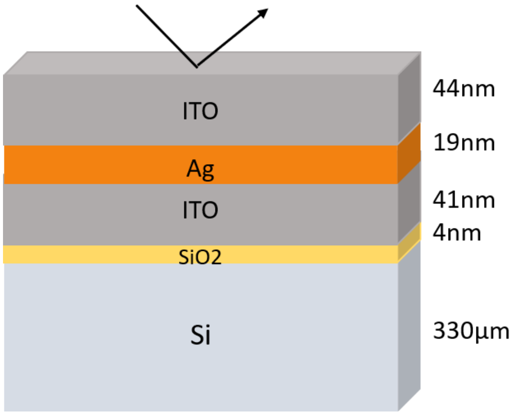


Fig 3. 4 schematic layer structure (ITO-Ag-ITO) coated on the silicon substrate.

Table 3-1 Obtained results from ellipsometry spectroscopy at the wavelength of 1110nm

Material	**Thickness**	**n**	**K**
Silicon	330 µm (Input)	3,53	4 ×10^{-3}
SiO₂	4 +/- 1 nm	1,45	--
ITO	41 +/- 1.6 nm	1,47	2,2×10^{-2}
Ag	19 +/- 1.2 nm	0,27	7,9
ITO	44 +/- 0.5 nm	1,47	2,2×10^{-2}

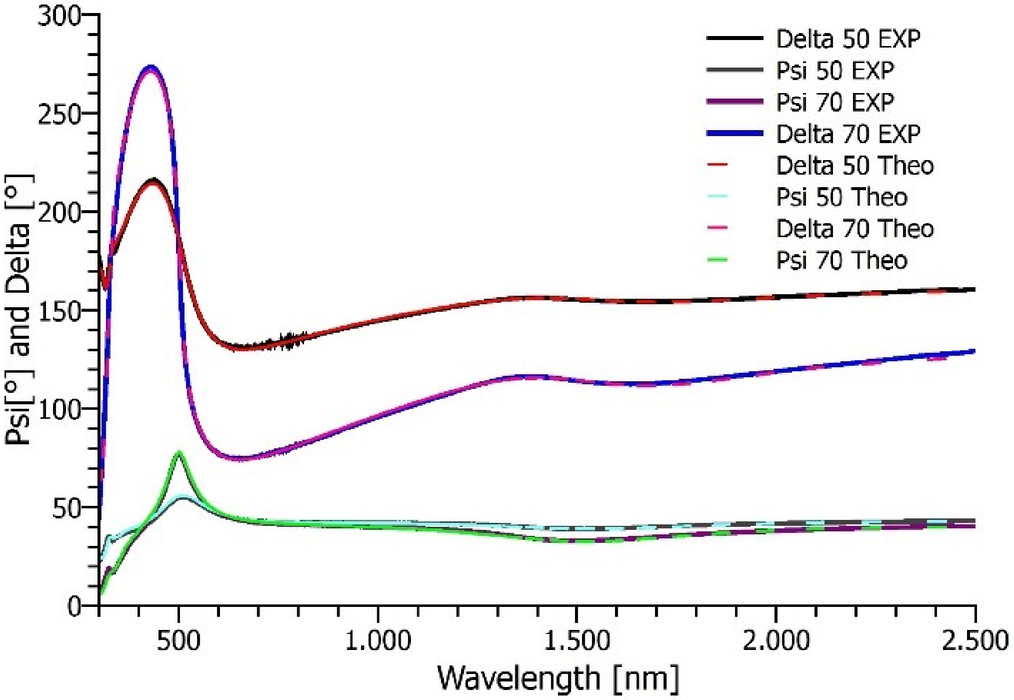


Fig 3. 5 Calculated and measured Psi and Delta of coated silicon at two angles of incidence of 50° and 70°.

The layer has also been characterized by ARTA spectroscopy. The ARTA measurement of the layer's reflectivity is only possible through the air-layer-silicon interface. The reflectivity of the structure from the airside using the data obtained from the Ellipsometry spectroscopy is calculated. The calculation is done by SENTECH software for s-polarized (S-P) and p-polarized (P-P) light in the angle of incidence range from 10°-70° and at a wavelength of 1110nm. Fig 3. 6 compares the results of ARTA measurements and the calculated one by SENTECH software. It can be seen that simulated reflectivity is in conformity with the measured reflectivity. This result indicates that the reflectivity inside the silicon complies with the SENTECH software calculations.

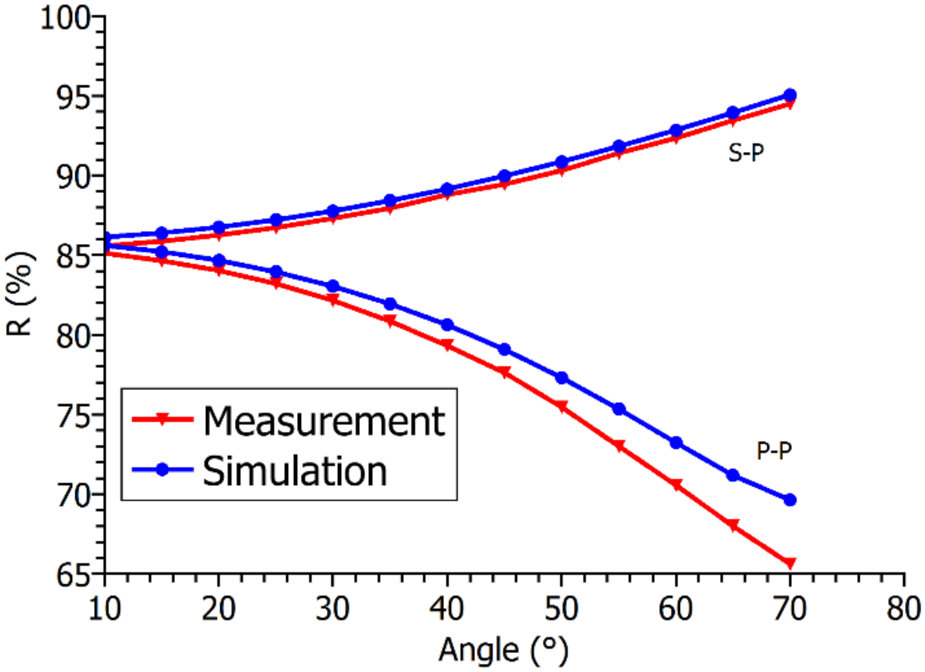


Fig 3. 6 Spectral reflectivity simulated (circles) and measured (triangles) as a function of AOI (at the range of 10°-70°) at a wavelength of 1110nm for S- polarized (S-P) and P-polarized (P-P) of light.

Fig 3. 7 compare angular dependence of light reflection inside the bare silicon and the coated silicon with ITO-Ag-ITO and illustrates how the coated layer changes the intensity of reflected light depending on the angle of incidence of light. So this layer can be a proper choice for protecting the IC backside.

Using the parameters obtained from ellipsometry, reflectance, transmittance, and absorbance of light at the wavelength of 1110nm are calculated according to the angle of incidence (0°-80°) inside the silicon which is coated with protection layer using the SENTECH software and the results are shown in Fig 3. 8. These curves illustrate that the reflectance changes over the angle of incidence and the variations of the reflectance are due to the variation of absorption over the angle of incidence and not the transmission. Only a slight part of the light, less than 8%, and only for the angle less than 16° transmits, and light is absorbed with in the coated layer by 5% to 50 % which depends on the AOI.

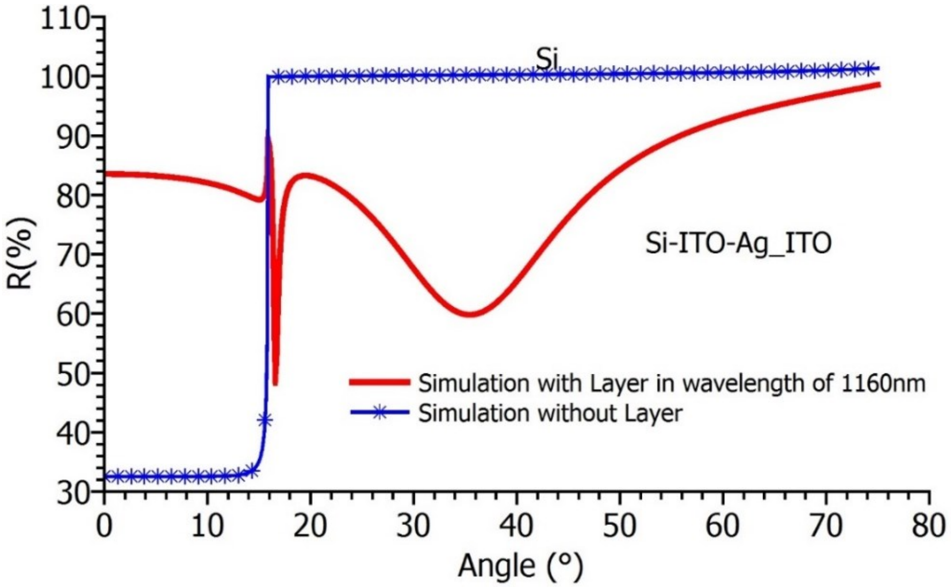


Fig 3. 7 Angular-dependent reflectance of the silicon (blue-stared line) and silicon coated with ITO-Ag-ITO (red line) in the infrared wavelength. The curves are calculated by the Sentech software, assuming the light source and the detector are located inside the silicon, on the opposite side of the layer.

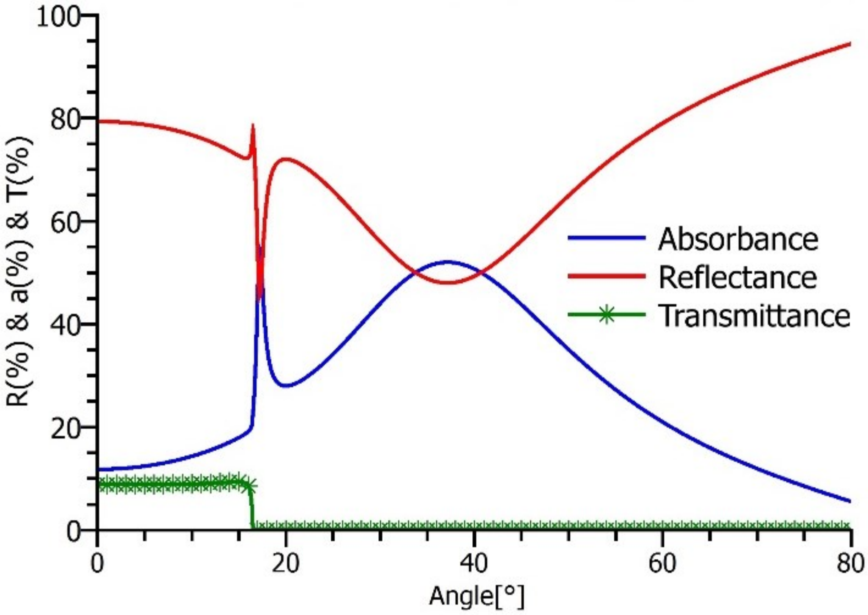


Fig 3. 8 The angular-dependent reflectance, transmittance, and absorbance of the light with the wavelength of 1110nm inside the coated silicon.

3-3 Deposition and characterization of TiO2-Ti-TiO2

The second optically active layer which provides angle-dependent reflectivity for the silicon interface in the near-infrared region, is a layer consist of a thin film of titanium (Ti) sandwiched between two layers of Titanium dioxide (TiO_2).

The films were prepared by radio frequency (RF) magnetron sputtering from a Ti target (3-inch diameter) at room temperature. The pure Ti thin film has been deposited at the sputtering power of 60W with argon as working gas. The TiO2 films were produced with an Ar/O2 gas mixture at the sputtering power of 180W. The layer has been coated on the backside of the chip and on an extra silicon wafer to have a sample to characterize the layer.

Spectroscopic ellipsometry was applied to determine the thickness of the coated layer. Psi and delta are measured at two angles of incidence for light source and detector (55° and 70°). The measured data are fitted to a model to extract the thicknesses and the optical constants of the layer. The TiO_2 layers are simulated using Tauc-Lorentz models, and the Ti layer is simulated using Drude-Lorentz models. The results based on data obtained with a Sentech SE 850 ellipsometer and simulated by Spectraray 3 software at the wavelength of 1110nm are outlined in Fig 3. 9 and Table 3-2. The thicknesses of the layers have been calculated using optical coefficients n (refractive index) and k (extinction coefficient) from the Sentech database.

The fitted and the measured ellipsometric delta and psi values are demonstrated in Fig 3. 10; the goodness of the fit is 99.4% (Mean square error = 0.6).

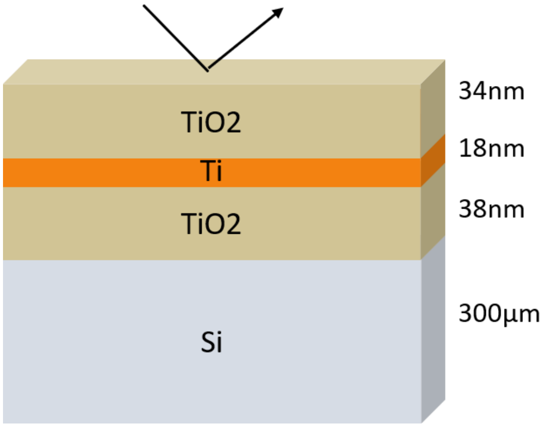


Fig 3. 9 schematic layer structure (TiO2-Ti-TiO2) coated on the silicon substrate.

Table 3-2 Obtained results from ellipsometry spectroscopy

Material	Thickness	n	K
Silicon	300 µm (Input)	3.53	4 ×10^{-3}
TiO_2	38 +/- 0.008 nm	2.59	--
Ti	18 +/- 0.008 nm	3.39	3.77
TiO_2	34 +/- 0.006 nm	2.59	--

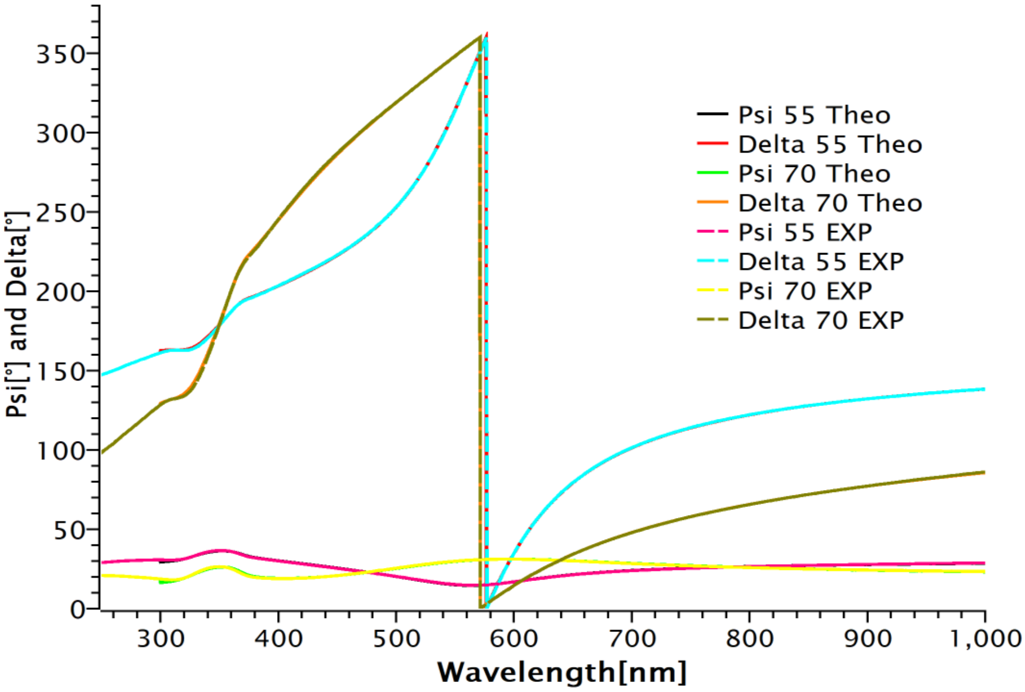


Fig 3. 10 Calculated and measured Psi and Delta of coated silicon with TiO2-Ti-TiO2 at two angles of incidence of 55° and 70°.

Cross-sectional scanning electron microscopy (SEM) of the coating on the silicon wafer is performed at an acceleration voltage of 10 kV. The SEM image is presented in Fig 3. 11. For this image, the silicon wafer is broken, and the cross-section of a piece of the wafer is used for SEM imaging. This SEM image shows that the thickness of the coating is about 85nm which consists of 40nm TiO_2 layer on the silicon wafer, 20nm of Ti, and 35nm of TiO_2 on top. The thicknesses shown in the SEM image are very close to the one obtained from Ellipsometry spectroscopy (Table 3-2).

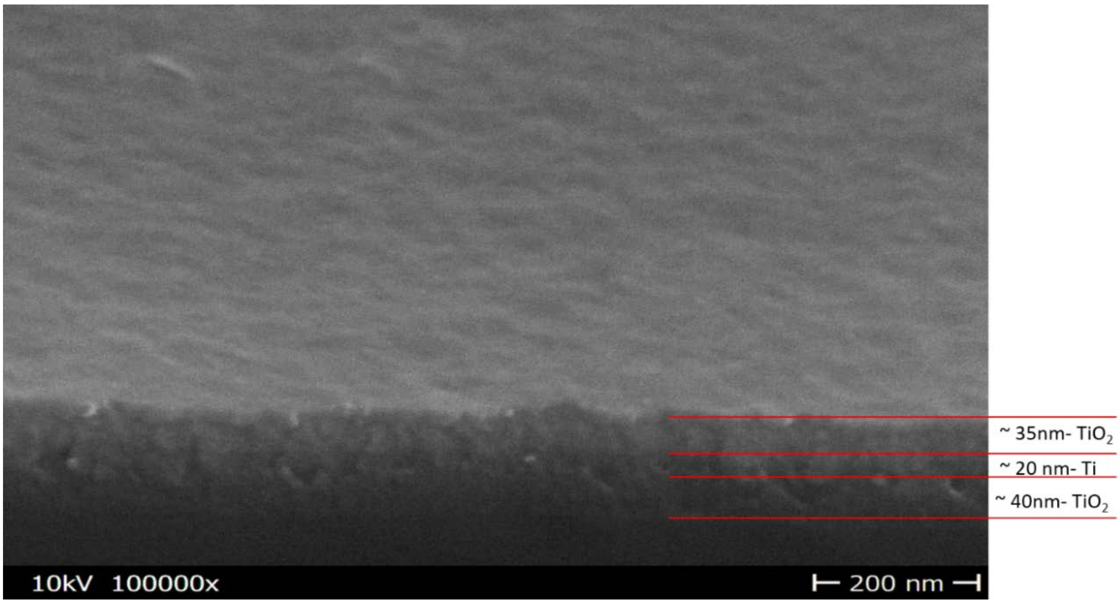


Fig 3. 11 Cross-section SEM image of the TiO2-Ti-TiO2 coated on the silicon wafer.

Regarding the parameters obtained from ellipsometry, the angle dependence of the reflectivity inside the silicon is calculated using the software SpectraRay 3 provided by Sentech at the wavelength of 1110nm. In Fig 3. 12, the reflectivity of light inside the silicon (blue stared line) and coated silicon with the layer (red line) are compared. Before coating the layer, the reflectivity for an angle of incidence larger than 16° was 100%. The result indicates a change to 11%-95% after coating the optical layer. Fig 3. 13 compares the reflectance, the transmittance, and the absorbance of the layer, when the light reaches the layer from inside the silicon. It is observable that the absorbance of the layer caused the reductions in the reflectance and there is no transmittance for the light with an angle of incidence larger than 16°. The layer reduced the transmission of the infrared light to 37% for the light with AOI of 0°-16°. The layer provides a strong angle-dependent reflectivity for the silicon surface. Therefore, this layer can be considered as an optically active layer for the protection mechanism.

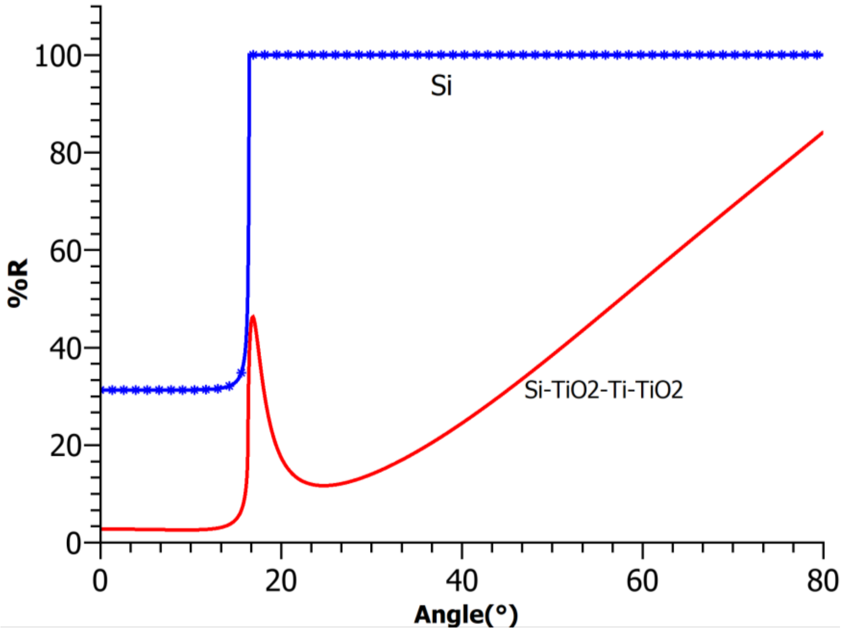


Fig 3. 12 Angular-dependent reflectance of the silicon (blue-stared line) and silicon coated with TiO_2-Ti-TiO_2 (red line) in the infrared wavelength. The curves are calculated by the Sentech software, assuming the light source and the detector are located inside the silicon, on the opposite side of the layer.

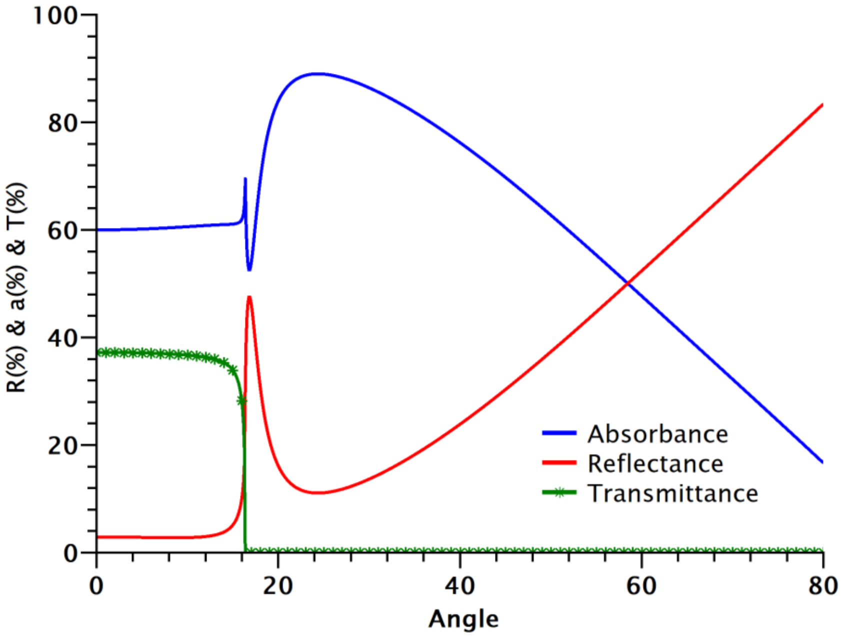


Fig 3. 13 The angular-dependent reflectance, transmittance, and absorbance of the light with a wavelength of 1110nm inside the silicon coated with TiO2-Ti-TiO2.

Both layers introduced as the optically active layer in this work provide angular-dependent reflectivity in the infrared region when coated on the IC backside. The layer consists of Ti gives more changes in reflectance over the angles while the layer consists of Ag provides less transmission in smaller angles. The reflectance of these two layers is compared in Fig 3. 14.

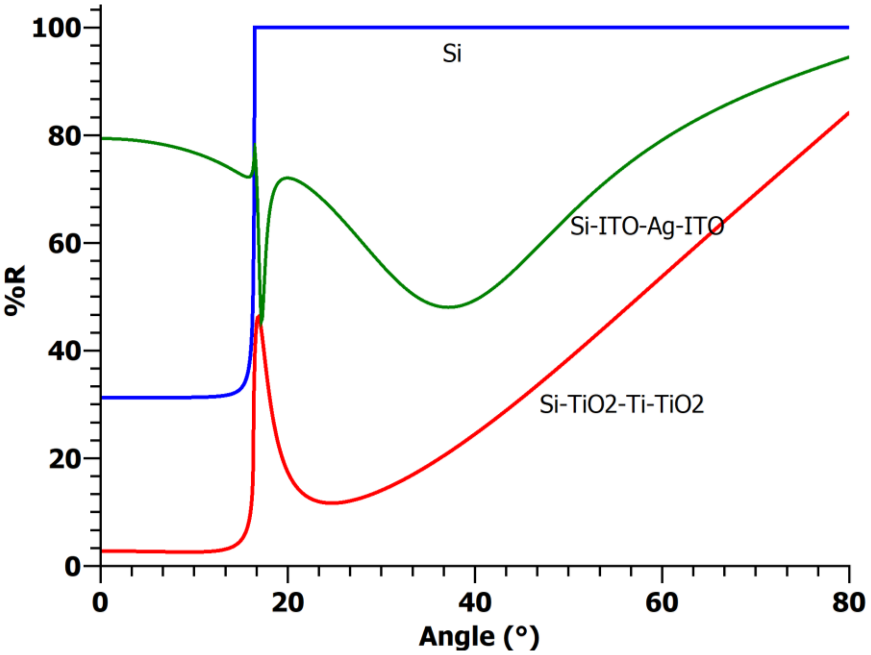


Fig 3. 14 Calculated Reflectivity of silicon back surface (blue line) and silicon coated with ITO-Ag-ITO (green line) and silicon coated with TiO2-Ti-TiO2 (red line) at a wavelength of 1110nm.

Chapter 4: Experiments, Results, and Discussion

This chapter presents the experimental procedure and the results of applying the two different optically active layers as the protection structure on the IC backside. In the first part, the concept of the method has been proved by applying a layer of ITO-Ag-ITO as a protection layer. After analyzing the results of the first experiment, a layer of TiO_2-Ti-TiO_2 was designed as the protection layer, and the test chip was redesigned to improve the method. Then the same procedure is repeated, and the results are presented in the second part. The results confirm the effect of the optically active layer coated on the IC backside on the intensity of the light reflected from the back surface. Changes in the intensity of light lead to a change in the photocurrent of the detectors.

In the following, the protection mechanism presented for the IC backside in this work is assessed, and the possible options to approach an appropriate protection structure are considered.

The results presented in this chapter have been published in [80], [81],[82], [83], and [84].

In this chapter, LE refers to the light-emitting device, which is a diffusion area in the silicon bulk of the test structure, and LED refers to a light-emitting device that is separate from the test structure.

4-1 ITO-Ag-ITO as the protection layer

As the first protection layer, a structure consisting of ITO-Ag-ITO has been coated on the IC back surface by an in-line magnetron sputtering system. Because the mentioned layer provides angle-dependent reflectivity, it can be a suitable choice for the protection mechanism. The deposition process and the result of the characterization of the layer are presented in the previous chapter. In this chapter, the attack detection ability of the protection mechanism using this layer is evaluated, and the results of the electrical measurements are discussed.

4-1-1 Device Under Test

The device used in this work was designed at Technische Universität Berlin (TUB) and produced in 250nm IC technology at IHp GmbH (Innovations for High-Performance Microelectronics, Leibniz-Institut für innovative Mikroelektronik) in Frankfurt (Oder), Germany. In this chip, the full circuitry covered an area of 0.5mm x 4mm. The chip was thinned out to a remaining silicon thickness of 330µm. The silicon surface was polished to create a surface without scratches and deformation. For this experiment, p-n junctions are designed as a light emitter and detectors. Due to the small dimensions of a single p-n junction, it was possible to distribute the structures over the entire area of the circuitry.

By knowing the location of the structure (light emitter and detectors) on the IC and thickness of the silicon bulk, the angle of incidence of light that will be absorbed by each detector can be calculated. Fig 4. 1 shows the IC cross-section where LE is a light-emitting device, and PD is a detector. Here, x is the distance between the LE and PD on the circuitry side of the IC, L is the length of light that passes from LE to the chip back surface and from the backside to the PD, α is the angle of incidence of light, and d is the thickness of the chip.

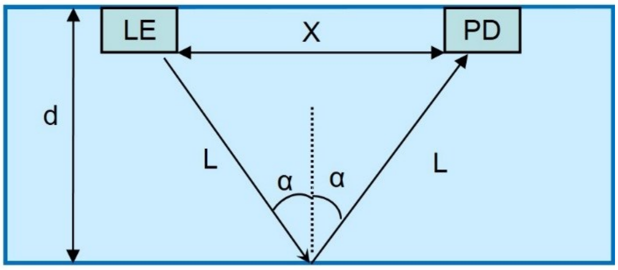


Fig 4. 1 Cross-section of the chip where light source (LE) and detector (PD) are located, x is the lateral distance between LE and PD, d is the thickness of silicon, α is the angle of incidence, and L is the path length of light before and after reflection.

In a right-angled triangle, the tangent of a non-right angle is defined by the ratio of the length of opposite side to the length of the adjacent side. Thus, here:

$$\alpha = \tan^{-1}\frac{x/2}{d}$$

x is known from the layout of the chip, and the thickness of the chip (d) is measurable, so the α for each detector can be calculated.

4-1-2 Experiments and results

In order to convenience in handling and preparation of the chip for coating the layer on the IC backside, the chip is mounted into a silicon wafer. For this purpose, a hole larger than the chip surface has been made in the silicon wafer to hold the chip; it allows access to the backside and front side of the chip. Fig 4. 2 shows the chip mounted into a silicon wafer. The chip has been kept in the middle of the hole with a UV curing adhesive, Vitralit UC 1609, which has a low viscosity and is a transparent adhesive [85]. The adhesive is found only between the sides of the chip and the silicon wafer (the holder); the circuitry side and the backside of the chip are not covered.

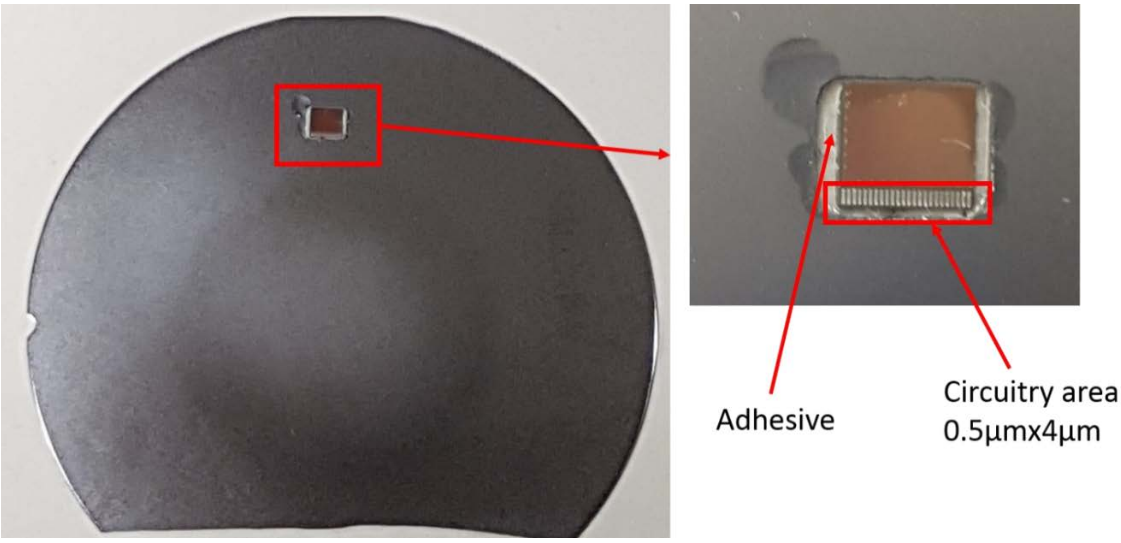


Fig 4. 2 Chip is mounted into a silicon wafer (frontside view). The device is kept in the hole with an adhesive.

To generate an optical signal inside the IC, a forward current of -5mA corresponding to a forward voltage of almost -1V is applied to a p-n junction, which is assigned to be a light-emitting (LE) device. The current-voltage (I-V) characteristic of the LE, which is an n diffusion in a p-doped silicon substrate, is displayed in Fig 4. 3.

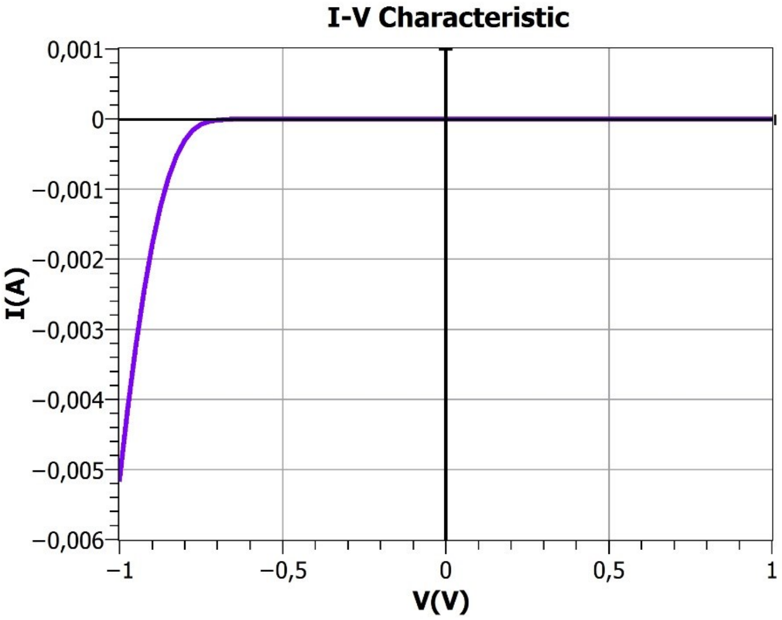


Fig 4. 3 I-V characteristic of a p-n junction under forward and reverse bias.

In order to detect the light reflected from the IC backside, nine p-n junctions in reverse bias operation are used as photodetectors (PD_1 - PD_9). The photodetectors are located at different intervals from the LE. Fig 4. 4 illustrates the schematic top-view of the device under test and the location of the light emitter (red rectangle) and detectors (blue rectangles). Detectors are located within a distance of 691µm to 2596µm away from the light emitter, which results in detecting the light with different angle of incidence (46.5°-75.8°). The distance between the LE and detector and the angle of incidence of the reflected light absorbed by the detector is calculated for each detector and represented in Table 4. 1

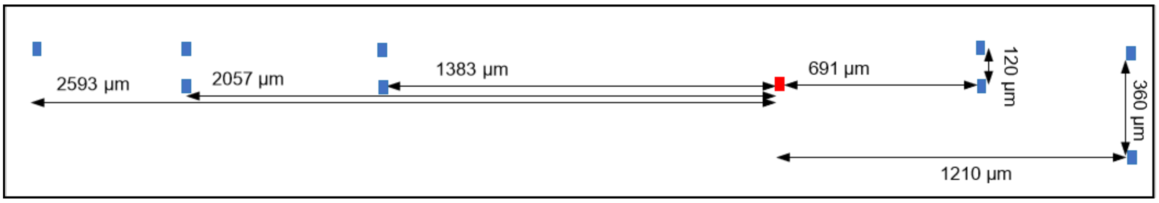
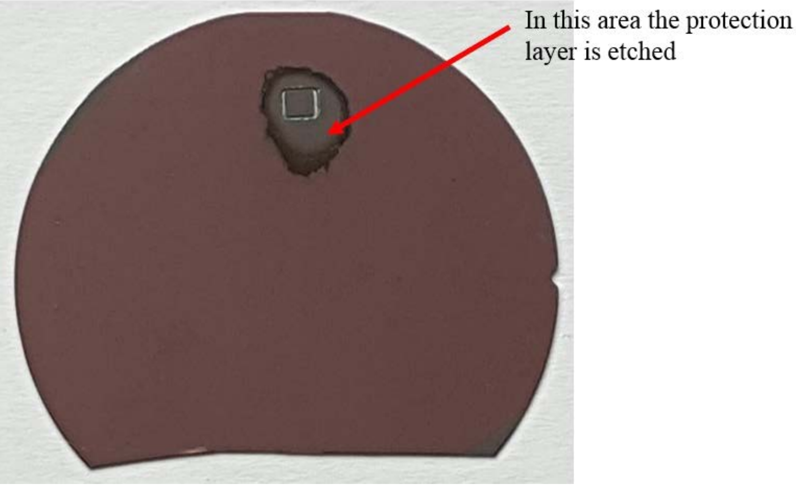


Fig 4. 4 Schematic top-view of the chip and the location of the light emitter (red rectangle) and detectors (blue rectangles). Light detectors and emitter are shown four times larger than actual scale.

Before coating the protective layer on the chip backside, a reverse voltage is applied to the detectors, and the dark reverse current (when the LE is off) and photocurrent (when the LE is on) of the detectors are measured. The dark current of all detectors was less than 1pA, while the reverse current of detectors under illumination increases by 3 to 7 orders of magnitude depending on the distance between the LE and detectors (872pA- 8.67µA). The photocurrent of each detector is presented in Table 4. 1 under the title of "I_{ph} (before coating)." The amount of dark current is small enough to consider the reverse current of the detectors under illumination as a photocurrent. In order to evaluate the reliability and repeatability of the measurements, the photocurrent of each detector is measured three times on different days; the changes were less than 5%, which confirms the reliability and repeatability of the measurements. The I_{ph} presented in Table 4. 1 is the average of the three measured currents. For electrical measurements on this chip, hp 4145A semiconductor parameter analyzer is utilized.

In the next step, an optically active layer consisting of ITO-Ag-ITO, with a thickness of 41nm for inner ITO, 44nm for outer ITO, and 19nm for Ag, was deposited on the IC back surface. The coating process and the results of the characterization are described in detail in the previous chapter. Then, in order to investigate the layer's effect on the intensity of the reflected light that leads to a change in the photocurrent of the detectors, the same electrical measurements are performed on the same structure as before. The dark current and photocurrent of detectors are measured. Again, the photocurrent of each detector is measured three times on different days, and the changes were less than 5%. The results are available in Table 4. 1 under the title of "I_{ph} (after coating)," (average of the three measurements). It can be seen that the photocurrent of the detectors is not any more equal to the initial photocurrent (before coating) and is reduced.

In the next level, the layer is removed from the back surface using chemical etching to have the same surface as before coating. The etching of layer is performed with a chemical solution of ferric chloride which is a mixed solution of HCl (37%): FeCl3 (40Be´) at 1.00: 1.00 [86]. The etching has been done through a drop method by using a cotton swab. Fig 4. 5 shows the mounted chip in a silicon wafer where the protection layer has been etched away from the chip's back surface; the layer is still on the rest of the wafer surface. To be sure that the changes in the photocurrent were only the effect of the protection layer, the same electrical measurements as before coating and after coating are carried out. The photocurrent of each detector is measured three times on different days; the changes are less than 5%. The photocurrent that is the average of the three measurements for each detector is presented in Table 4. 1 under the name of I_{ph} (after etching).



In this area the protection layer is etched

Fig 4. 5 Chip is mounted into a silicon wafer; the protection layer is etched from the chip backside and the area around.

The reverse current of one example of our detectors (PD4) has been demonstrated in Fig 4. 6, indicating almost no dependence of the voltage in reverse operation. Id (red line) is the dark current when there is no illumination, I_{ph} is the photocurrent when the chip is protected by the layer, represented by the blue line with points, and the green line with triangles represents when the layer is removed.

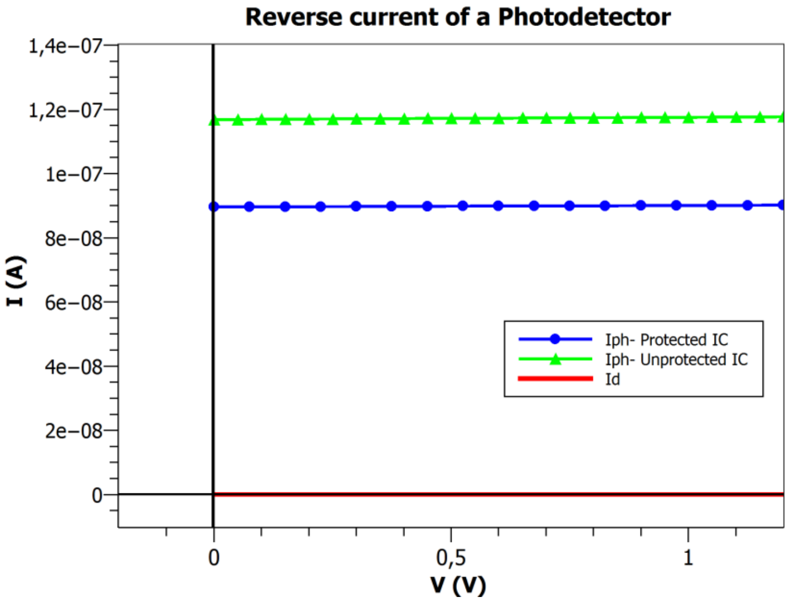


Fig 4. 6 I-V characteristic of a photodetector (PD4), which detects light with AOI 62° and is located at a distance of 1233µm from the LE. The red line represents the dark current, the blue line (circles) represents the photocurrent of the detector when the IC is protected by an optically active layer, and the green line (triangles) represents I_{ph} when the layer is removed from the IC backside.

Table 4. 1 describes the results of the performed experiments, photocurrent of photodetectors (PDs) before coating the layer, after coating the layer, and after etching the layer. The table also exhibits the distance between the LE and PDs, the percentage of the changes in photocurrent that is caused by the layer for each detector, and the percentage of the reduction in reflectance caused by the layer. The angle of incidence of the light presented in Table 4. 1 is the angle at which each detector absorbs the light reflection (α in Fig 4. 1).

Results state that photocurrents decrease by 15% to 25% after depositing the layer and almost return to the initial amount (before coating) after removing the layer. For example, the photocurrent of PD3, which detects reflected light at the angle of 61.7°, before coating the layer was 69.7 nA and 53 nA after coating and 68.9 nA after removing the layer. The reduction is clearly identified with a 24% difference. This is in rough accordance with the simulated difference of 18%.

The results of the experiments are graphically illustrated and compared in Fig 4. 7. The blue dashed line highlights the reflectance of the bare silicon at a wavelength of 1110nm and for the angle of incidence (AOI) range of 0-90°. The black dashed line is the reflectance of the silicon coated with the mentioned layer, which shows how this layer modifies the reflected light and changes depend on the AOI. The purple stars represent the initial photocurrent of the detectors, $I_{ph,}$ before coating the layer. In order to compare the changes in the photocurrent with the changes in the intensity of the reflected light from the backside, the photocurrents are presented as percentages. When the silicon backside is bare, reflectance in angles larger than 16° is 100%. Since the current through photodetectors is directly proportional to the intensity of the incident light, the initial photocurrent is classified as 100% for each detector in any distance with AOI>16°. The red and green stars are the percentage of the photocurrent of the detectors after coating the layer and after removing the layer respectively relative to the initial amount.

Table 4. 1 Photocurrent of detectors before and after coating and after removing the optical layer in 1V reverse bias, AOI of the light at the back surface and distance between LE and the detector.

Detectors	I_{ph} (before coating)	I_{ph} (after coating)	I_{ph} (after Etching)	Distance between LE & PD	Angle of incidence of light [°]	%change of I_{ph} caused by protection layer	%change of intensity of light from model
PD1	8,67 µA	7,41 µA	8,8 µA	691µm	46,5	15%	40%
PD2	5,12 µA	4,16 µA	5,10 µA	702µm	47	18%	40%
PD3	69,7 nA	53 nA	68,9 nA	1216µm	61,7	24%	18%
PD4	118 nA	88,8 nA	117,5 nA	1233µm	62	25%	17%
PD5	285 nA	220 nA	278 nA	1382µm	64,5	23%	15%
PD6	107 nA	84,2 nA	104,5 nA	1388µm	64,7	21,5%	15%
PD7	6,12 nA	4,95 nA	6,04 nA	2074µm	72,4	19%	9%
PD8	3,07 nA	2,48 nA	3,02 nA	2078µm	72,5	19,1%	9%
PD9	872 pA	708 pA	862 pA	2596µm	75,8	18,8%	7%

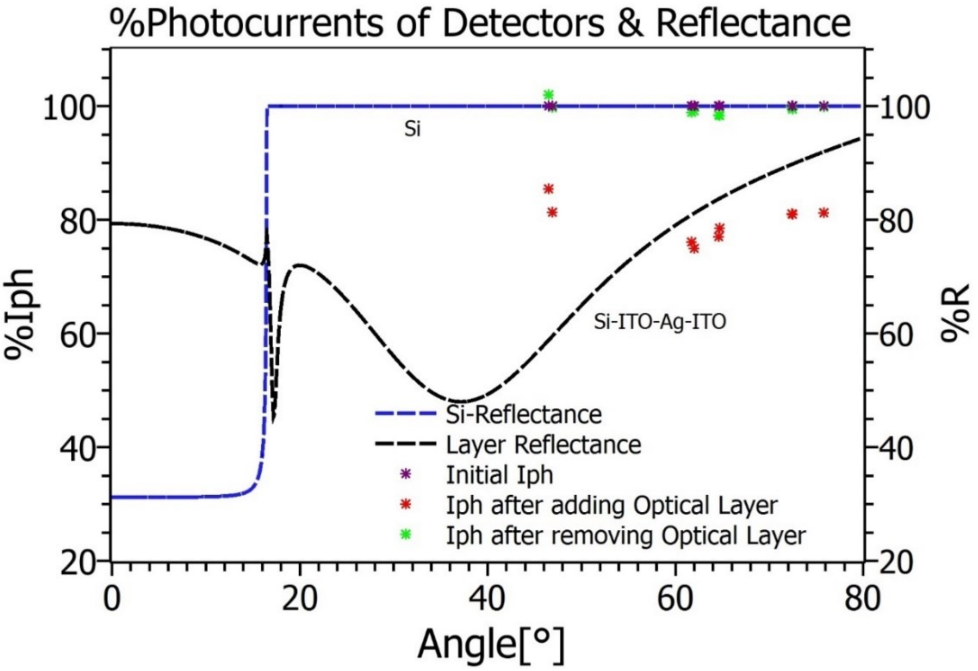


Fig 4. 7 Percentage of photocurrent of the detectors (Iph) before deposition of the optical layer (purple stars- Initial Iph), after deposition (red stars), after removing the optical layer (green stars), the calculated angular-dependent reflectivity of coated silicon (black dashed line) and uncoated silicon (blue dashed line) at the wavelength of 1110nm. [81]

The results obtained from this experiment prove the protection concept and express that it is a promising method to reach a secure IC. In Fig 4. 7 it can be seen that the changes in photocurrent of the detectors with different AOI, in the presence of the protection layer, are so close. These amount of changes in photocurrent versus angles may not be enough to take advantage of the angle-dependent reflectivity of the layer. Therefore, to improve the technique, the layer should be replaced with a film that provides stronger angle-dependent reflectance. A thin film of Titanium (Ti) sandwiched between two layers of Titanium dioxide (TiO_2) brings it closer to the goal. In the next section, the use of the mentioned layer for the protection mechanism is investigated.

4-2 TiO_2-Ti-TiO_2 as the protection layer

The second thin film that is suitable for the protection mechanism is a film consisting of TiO_2-Ti-TiO_2. This layer coated on the silicon surface provides strong angle-dependent reflectivity over the infrared region. This layer is coated at room temperature on the IC backside. The deposition process and results of the characterization are described in the previous chapter. In the following, the defense mechanism when this layer is used as a protection structure is evaluated.

4-2-1 Device Under Test

The device that is used for this experiment was designed at Technische Universität Berlin (TUB) and produced in 250nm IC technology at IHP GmbH (Innovations for High-Performance Microelectronics, Leibniz-Institut für innovative Mikroelektronik) in Frankfurt (Oder), Germany.

The circuitry side covers an area of 1mm×2mm. The structures used in this work are general p-n junctions that are distributed over the entire area (1×2 mm^2). Each p-n junction is an n-diffusion with an area of 8µm×20µm and a doping level of 10^{20} /cm^3 in a p-doped silicon substrate. In this device, an n-well in the form of a square ring has been designed around three p-n junctions that are assigned to be used as the light emitter. The surrounding n-well is an n-diffusion of 50×50μm^2 with a thickness of 3µm and a doping level of 10^{17} /cm^3. Later in this chapter, its reason is explained. P-n junctions are placed at various intervals from the p-n junction and are assigned as the light emitter to have detectors with different angles of detection. The schematic top-view of the structures is illustrated in Fig 4. 8. The red rectangles with a blue ring around present the light emitter, and the other red rectangles illustrate the photodetectors. This figure contains the distances between light emitter number 1 and all other structures. To facilitate the handling and preparation of the chip for the coating and polishing process, the chip was diced in a larger size of 2.3mm × 6.2mm, where the structure placed in the middle of the die. In order to have a chip back surface without roughness and scratches, the chip was thinned and polished to a remaining silicon thickness of 300µm.

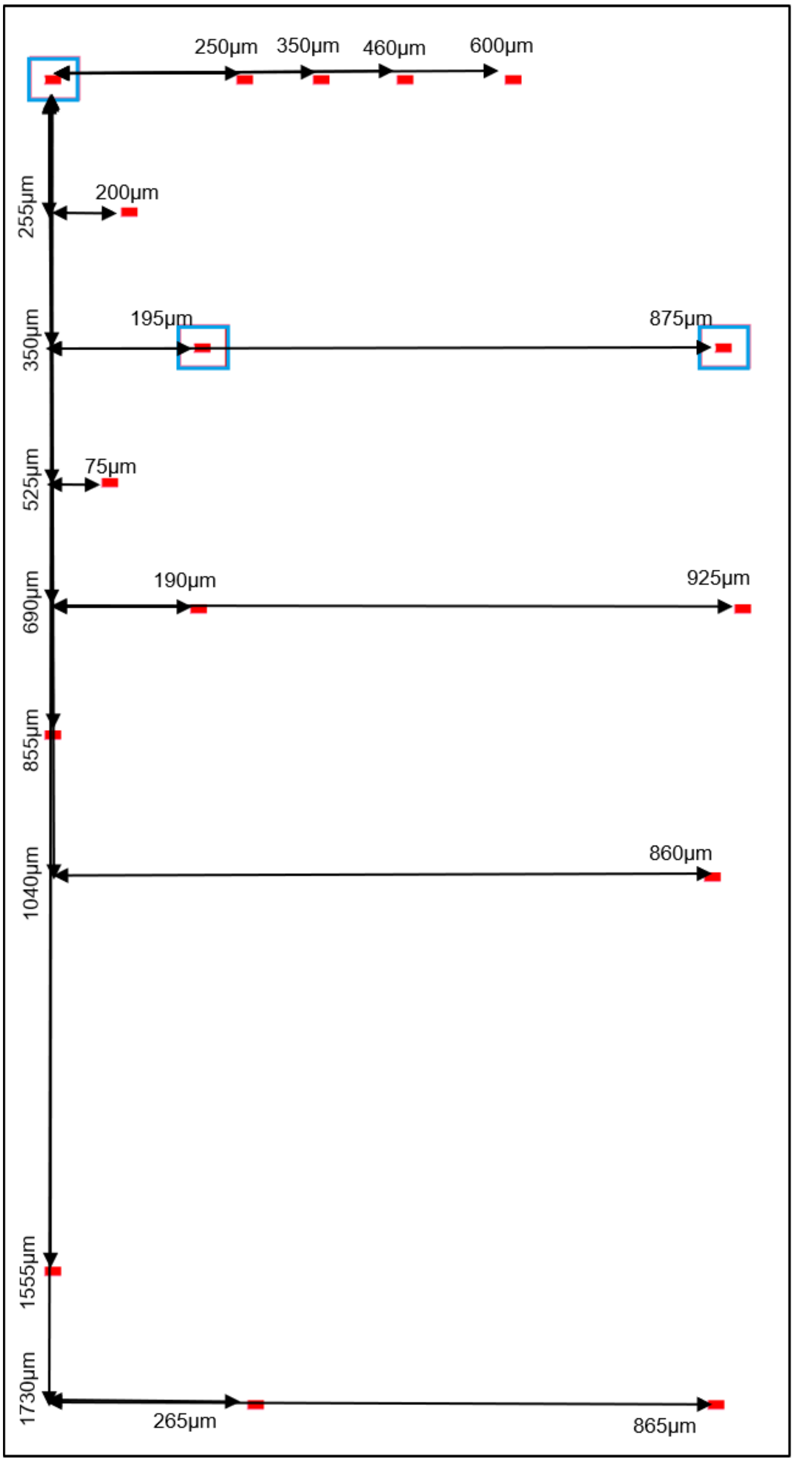


Fig 4. 8 Schematic top-view of the chip and the location of the light emitters (red rectangles with a blue ring around) and detectors (red rectangles).

4-2-2 Experiments and results

After thinning and polishing the silicon back surface, a thin film of 15nm Ti sandwiched between two layers of TiO_2 (each 40nm) is deposited on the IC backside. The deposition process and the characterization of the layer are presented in the previous chapter. In the next step, the chip is mounted onto an IC adapter and bonded to the adapter. The IC adapter that is used in this work was a QFP64, p=0.80 mm RM 2,54 mm from Roth Elektronik (RE966-01E) [87].

In order to access the IC backside, a hole with a size of 4×8 mm^2 (a bit larger than chip) has been made in the middle of the IC adapter and hold the chip in this hole with a tape on IC backside. It has shown in Fig 4. 9.

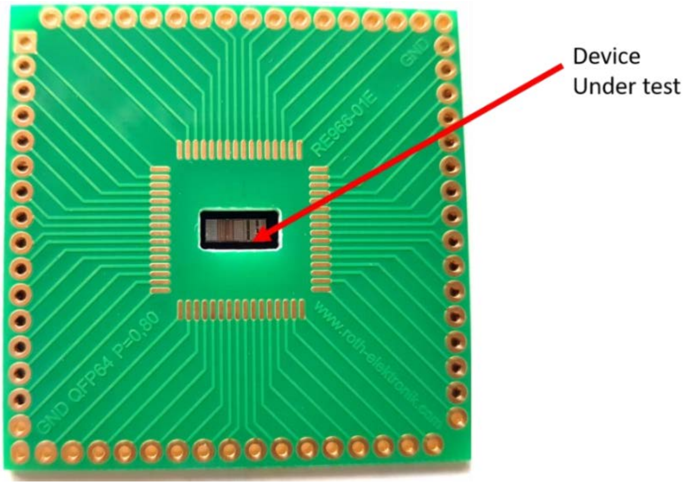


Fig 4. 9 IC adapter (QFP64) and the chip that is placed in a hole in the middle of the IC adapter.

The IC components (p-n junctions) are bonded to the adapter's connection pads, and afterward, the hole of the adapter and surroundings the wires are filled with filling material. The adhesive materials used in this work were Structalit 5893 and Structalit 5891 [88]. To contact the structure for electrical measurements, the pins are soldered to the adapter holes. The frontside and the backside of the chip mounted into the IC adapter are shown in Fig 4. 10 Now the IC back surface is exposed, and removing the layer is possible.

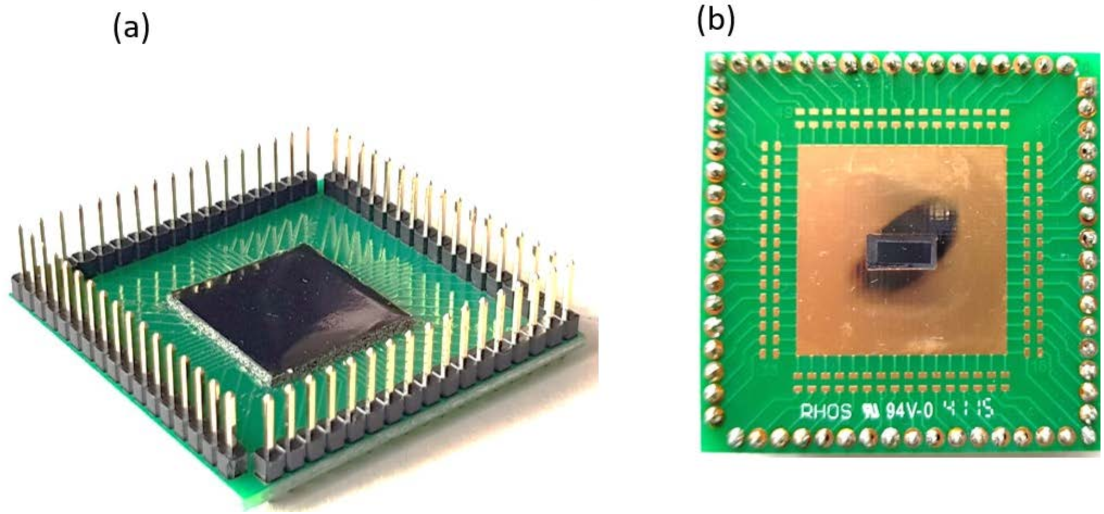


Fig 4. 10 (a) Frontside and (b) the backside of the chip bounded into the IC adapter. The pins are soldered to the adapter to contact the IC structure for electrical measurements.

To check the ability of the mechanism to detect the attack, which leads to remove or damage the layer, the photocurrent of detectors is measured in the presence and absence of the layer. For electrical measurements on this chip, Keithley 4200A-SCS parameter analyzer is utilized.

First, the dark current (I_d) of the detectors in reverse bias operation is measured when there is no emission in the IC. The dark currents of PDs are negligibly small, PDs show the reverse bias saturation currents of the order of 10^{-13} A.

In this work, one p-n junction was forward biased (-5mA (~ -0.9V)) as a light emitter (LE). The other p-n junctions that are located at various intervals from LE were used in reverse bias operation as photodetectors. The photocurrents were measured, and the amount of currents at 1V reverse voltage is recorded in Table 4. 2 under title of I_{ph} when the backside is protected. Measuring the photocurrent of the detectors is repeated three times for each p-n junction on different days to evaluate the reliability and repeatability of the measurements; the changes between the photocurrents of each PD were less than 5%, which confirms reliability and repeatability of the measurements. The photocurrents presented in Table 4. 2 are the averages of three measured values and are in the range of nA and μA. The photocurrents are 4 to 7 orders of magnitude higher than dark currents depending on the distance between the LE and detector. A comparison of the photocurrent of the detectors illustrates that when the light path length in silicon bulk increases, there is more absorption, and the intensity of the incident light at detectors decreases, and consequently, the photocurrent decreases.

In the next step, the protection layer is removed from the backside of the chip. In order to have the same surface as before, the layer is removed by chemical etching. A solution of $NaHCO_3$+H_2O_2 has been used for removing the layer from the backside of the chip.

After removing the protective layer from the IC backside, the same electrical measurements are performed, and again, the measurements are repeated three times. The averages of the photocurrents are represented in Table 4. 2 (I_{ph} - exposed backside). All electrical measurements are performed in a dark box. The results of the electrical measurements are represented in Table 4. 2.

The percentage of the changes in photocurrent that were caused by the optically active layer is calculated and shown in Table 4. 2:

$$\%\, changes\ of\ Iph\ caused\ by\ layer = \frac{Iph\_exposed\ backside\ - Iph\_protected\ backside}{Iph\_exposed\ backside} \times 100$$

This table also represents the distance between the LE and PDs, the AOI of light absorbed by each PD, the path length of light between the LE and each detector, and percentage of changes in reflectance at silicon back surface that shows how much the reflectance is reduced after coating TiO_2-Ti- TiO_2.

The results of the measurements (percentage of the photocurrent (%I_{ph}), and reflectivity (%R) in the absence and in the presence of the optical layer) are illustrated in Fig 4. 11. When the IC backside is exposed, the reflectivity is 100% for all angles larger than 16°. Since there is a direct proportion between light intensity and photocurrent, the photocurrent of each detector in the absence of the layer is classified to 100% (initial photocurrent). Then the percentage of the photocurrent after coating the layer is defined relative to the initial photocurrent.

The results indicate that the photocurrent of the detectors reduces after applying the protection layer, and the reduction depends on the AOI of light that is absorbed by detectors. The changes in photocurrents are in good agreement with the changes in the reflectivity. The changes in reflectivity result in a change in the intensity of the reflected light. The results confirm that the detectors absorb the reflected light from the backside and that the coated layer changes the intensity of the reflected light, affecting the photocurrent of the detectors. Therefore, the integrity of the back surface can be verified by measuring the photocurrent of the detectors.

It should be mentioned that in this experiment, all three light emitters and all available detectors on the IC were involved in the measurements, but because of degradation, only one LE and a few detectors survived until the end of the experiment. The reasons for degradation can be: 1) this chip was a prototype, and there was no ESD protection for devices. 2) all measurements are performed externally and through a long cable. In order to have a strong enough signal on the detectors, a voltage higher than power needed in real IC application is applied to the light emitter, which could have led to degradation.

Table 4. 2 Results of the electrical measurements photocurrent of the detectors in presence and absence of the optical layer in 1V reverse bias, AOI of the light absorbed by detector horizontal distance and pathlength of light between the LE and the PDs

Photo Detectors (PD)	AOI (α) [°]	Distance from LE (µm)	Light path length (2L) (µm)	I_{ph} - exposed backside	I_{ph}- protected backside	% changes of I_{ph} caused by layer	% changes of R caused by Layer
PD1	19	212	646	2,48µA	1,46µA	41,1	67
PD2	29,1	340	698	1.289µA	281,9nA	78	83
PD3	41,5	541	815	183,55nA	59,9nA	67,3	69
PD4	63,4	1220	1,364	18,57nA	12,63nA	32	38
PD5	66,1	1381	1,510	3,09nA	1,98nA	36	35

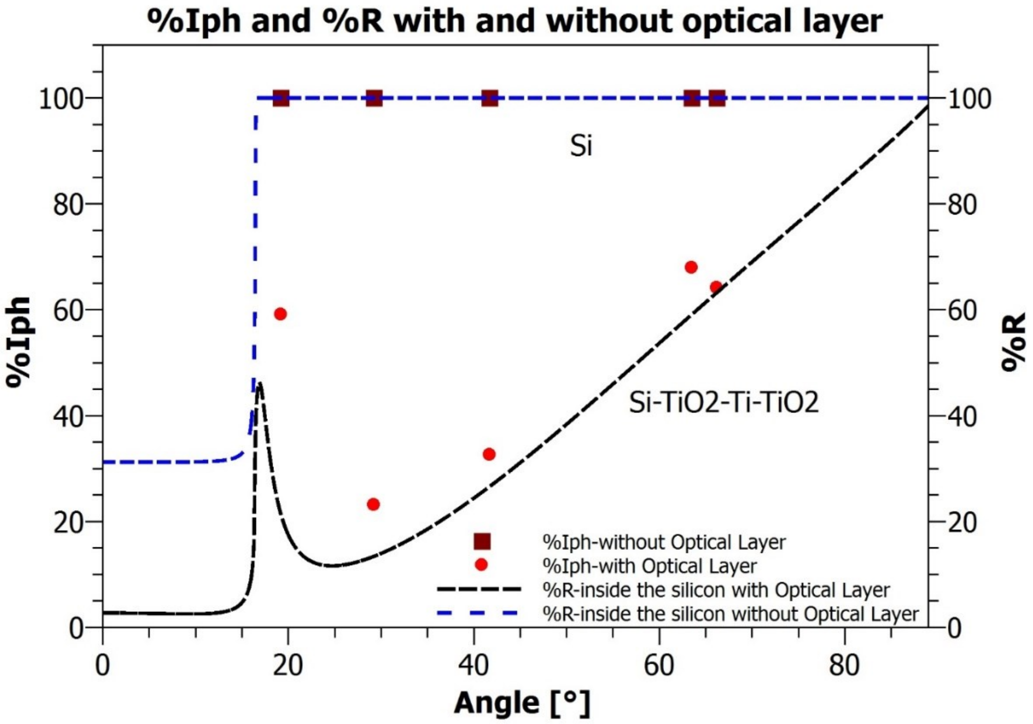


Fig 4. 11 Percentage of photocurrent of the detectors (I_{ph}) in the presence of the optical layer (red dots), in the absence of the optical layer (brown squares), the reflectivity of the silicon (blue dashed line), and the silicon coated with TiO_2-Ti- TiO_2 (black dashed line)

In order to protect the chip against optical attacks, the protection structure should be opaque to the light that silicon is transparent to (IR light). The opaqueness of the layer is investigated by calculating the transmittance. Fig 4. 12 displays the calculated transmittance of the bare silicon (black line) and silicon coated with TiO_2-Ti-TiO_2 (red line) when the light is emitted inside the silicon. If the light incident with an angle of incidence smaller than 16°, transmittance of the silicon-air interface is about 70%, and this amount is reduced to 36% when the silicon is coated with the protection layer. However, this layer reduces the transmission of the light but is not opaque enough. Therefore, it is necessary to deposit another layer that is capable of making the IC backside opaque. Applying a thin layer of Ag (silver) -about 100nm- sandwiched between two stacks of ITO -20nm for each stack- on the protection structure mentioned above can make this layer quite opaque and protect the IC against optical attacks as well.

In Fig 4. 12, the green line reveals that there is no transmission of the IR light after adding the Ag layer. Fig 4. 12 and Fig 4. 13 show the transmittance when the light is emitted from inside the silicon (in the case of measuring the photoemission of the structures) and when the light reaches the protected silicon from the outside (in the case of laser injection) respectively. The green line in both cases illustrates that the layer is opaque and tracking the emitted photon from the IC structure as well laser injection is not possible unless the protective layer is removed. The added layer affects the reflected light, and the removal of this layer can be detected by the detectors as well. The reflectance of the coated silicon with this layer is illustrated in Fig 4. 14. A thin film of Ag sandwiched between two layers of ITO is one example, any layer opaque to the IR can be an option for this job. The reflectance and transmittance are calculated using Sentech software.

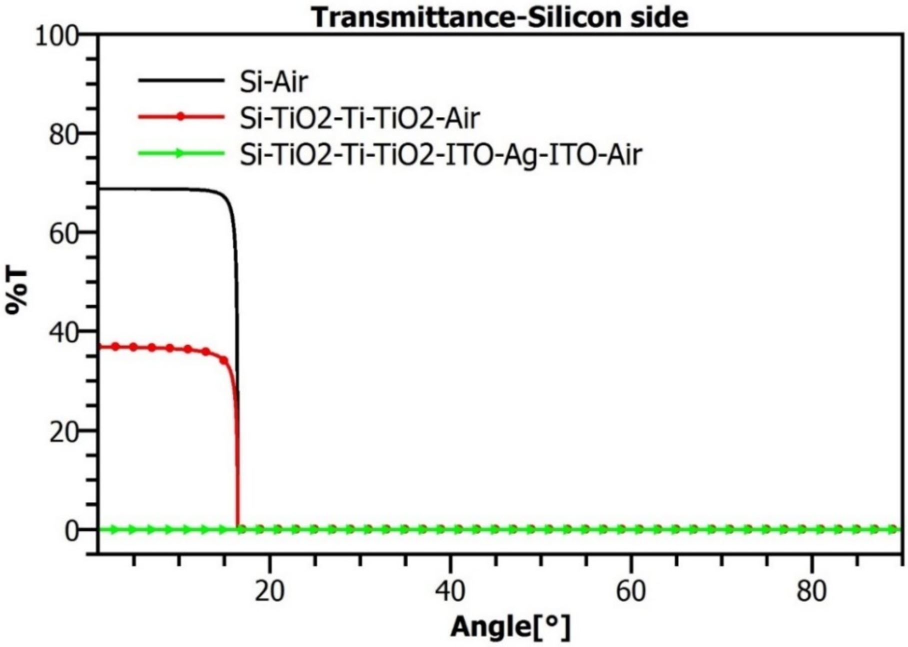


Fig 4. 12 Transmittance of the silicon (black line), silicon coated with TiO2-Ti-TiO2 (red line), and the silicon coated with TiO2-Ti-TiO2-ITO-Ag-ITO (green line) for the light at a wavelength of 1110nm emitted inside the silicon. The curves are calculated by the Sentech software.

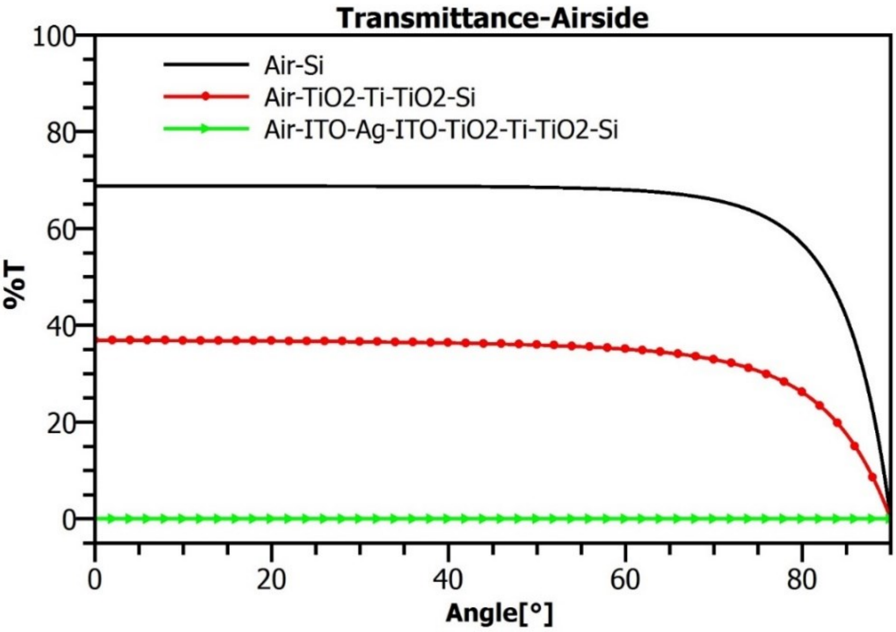


Fig 4. 13 Transmittance of the silicon (black line), Transmittance of the silicon (black line), the silicon coated with TiO2-Ti-TiO2 (red line), and the silicon coated with TiO2-Ti-TiO2-ITO-Ag-ITO (green line) for light at a wavelength of 1110nm emitted on the airside side. The curves are calculated by the Sentech software.

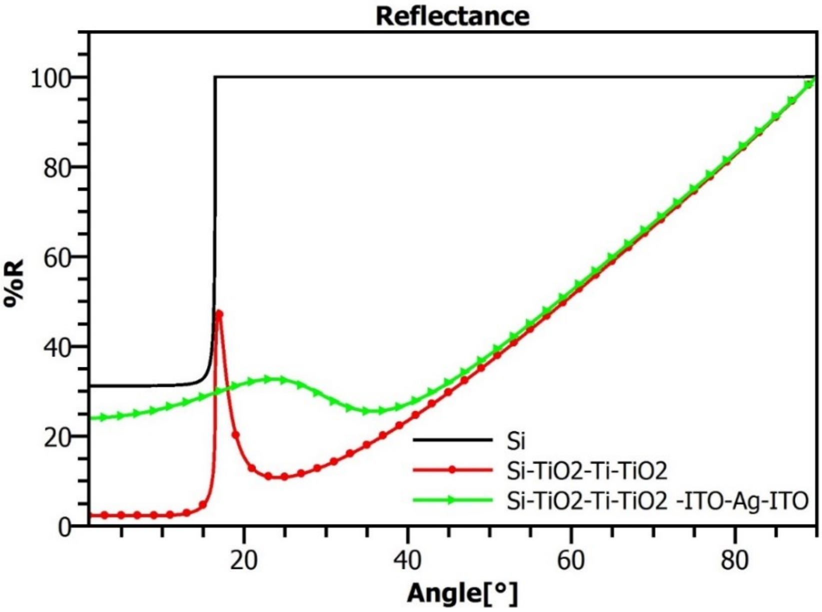


Fig 4. 14 Angle-dependent reflectance of the silicon (black line), silicon coated with TiO2-Ti-TiO2 (red line), and the silicon coated with TiO2-Ti-TiO2-ITO-Ag-ITO (green line) for the light at a wavelength of 1110nm emitted inside the silicon. The curves are calculated by the Sentech software, assuming the light source and the detector are placed inside the silicon, on the opposite side of the layer.

4-3 Discussion on the light source and the detectors

The light source that is used in this protection mechanism is a high-doped silicon p-n junction, and the generated photons have energy close to the silicon bandgap (1.1 eV). Besides the fact that silicon is not an efficient light emitter as it is an indirect bandgap semiconductor, the generated photons are partly absorbed by silicon bulk before reaching the detectors. Therefore, it is necessary to apply high forward bias to the light emitter to get enough light at the farthest detector.

The first issue that came up in the experiment was the degradation of the transistor whose drain was used as light emitter. When a high forward bias was applied to the drain, a large number of the carriers injected into the device and damaged the gate of the transistor. To overcome this issue an individual p-n junction is designed in the test device (the device used in the first experiment) and utilized as the light emitter.

Another issue with the light source is that when a high forward bias applied to the emitter, it may create a leakage current that travels in parallel with the light. When the light travels a long distance, this current is insignificant, but when the detector is close to the light source, the current cannot be ignored. The next issue is that the light source emits in all directions; hence, some radiation can travel directly from the emitter to the detectors. This radiation has no interaction with the backside, so it does not carry any information on the backside.

To prevent such problems, a structure like an n-well, here called guard ring (GR), is designed around the light source. Fig 4. 15 displays (a) cross-section and (b) top view of this structure (GR) around a p-n junction that is assigned as a light emitter (LE). This guard ring partially restricts the direct passage of light between the light-emitting and light-sensing devices and decreases the leakage current. Therefore, detectors detect mostly the reflected light from the back surface. Furthermore, the guard ring helps to keep the regular IC structure close to the light source safe from the side effects of driving a p-n junction in a high forward bias.

In the test structure used in the second experiment, the GR is designed and fabricated around the light source. The guard ring should be connected to the ground when the light source is on. In this test device, the guard ring around the LE is an n-well in the form of a square ring with a size of 50×50 μm^2 where the LE is centered within the GR. So, the total area of each light emission spot (LE + GR) is about 50×50 μm^2. The LE is made with a size of 20×8μm^2.

Depending on the thickness of the chip and the area that should be covered, it may be required to use more than one light emitter to check the integrity of the layer on the whole area of the chip backside. The drain or the source of any available transistor may be used as the light-sensing device.

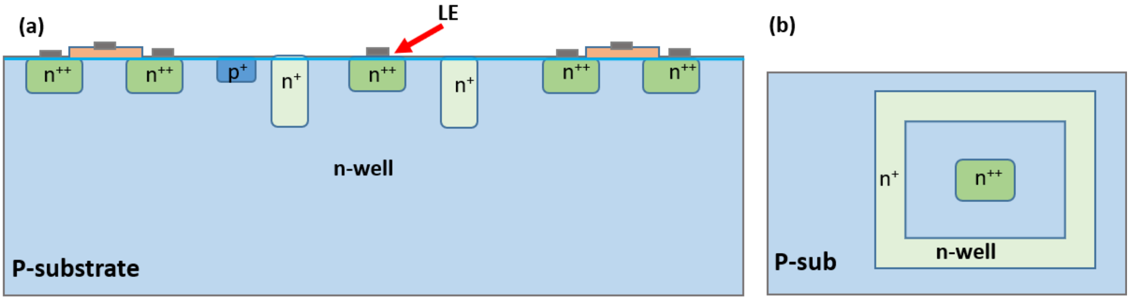


Fig 4. 15 Cross-section (a) and top view (b) of the light emitter (LE) and n-well (guard ring-GR) around the LE.

Another issue on the LE is that the light emitter should not be operated in a well. Since the well is heavily doped compared to the silicon bulk (substrate), more absorption happens in the well. Besides, this well-bulk junction can also act as a detector. For that reason, some parts of the created photons will be absorbed by the well and the junction. Fig 4. 16 shows the cross-section of a light emitter in a well. Light intensity (red arrows) decreases after passing through the n-well and the n-well-substrate junction.

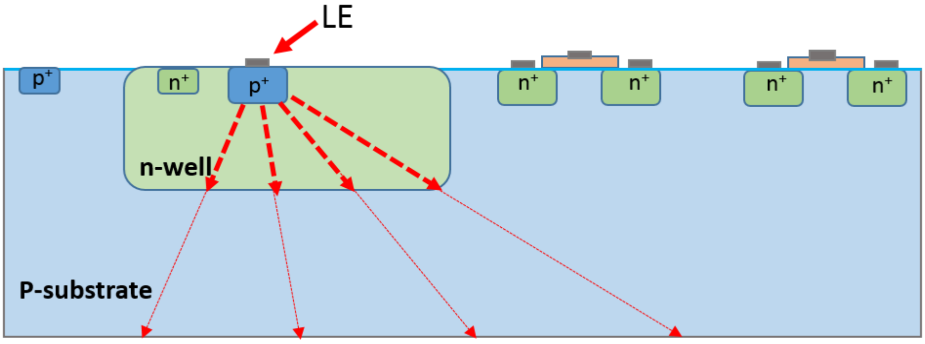


Fig 4. 16 Cross-section of the light emitter in an n-well. A p-n junction in a well is not the right choice for light emission.

In this technique, it is recommended that at least three detectors be used at different intervals from the light-emitting device to provide different angles of detection. This is required to make a pattern of the ratio of the photocurrent of the detectors (signals of the detectors) to check the integrity of the protection layer. For example, for a chip with a thickness of 50µm which has angles of incidence of 25°, 45°, and 65°, should have detectors at the distances 47µm, 100µm, and 215µm respectively from the LE. These distances change to 280µm, 600µm, and 1287µm for a chip with a thickness of 300µm.

Since the protection layer on the chip backside is opaque, an attacker needs to remove the protection layer to find the location of the stored secure data. Removing the layer results in disabling the device. It is assumed the attacker knows where the sensitive data is stored on the chip and only needs to remove the layer underneath of the sensitive devices. Therefore, it is essential to choose detectors in a way that at least one detector absorbs the reflected light on the silicon backside underneath of each sensitive device area. Fig 4. 17 and Fig 4. 18 show the top-views and cross-sections of the location of LE and detectors (PDs). It illustrates that the light emitter should be placed in a location that provides different intervals from intended sensitive device areas to give various angles of detection. It may require more than one detector to protect a device if the sensitive area is large (Fig 4. 17, S-D2).

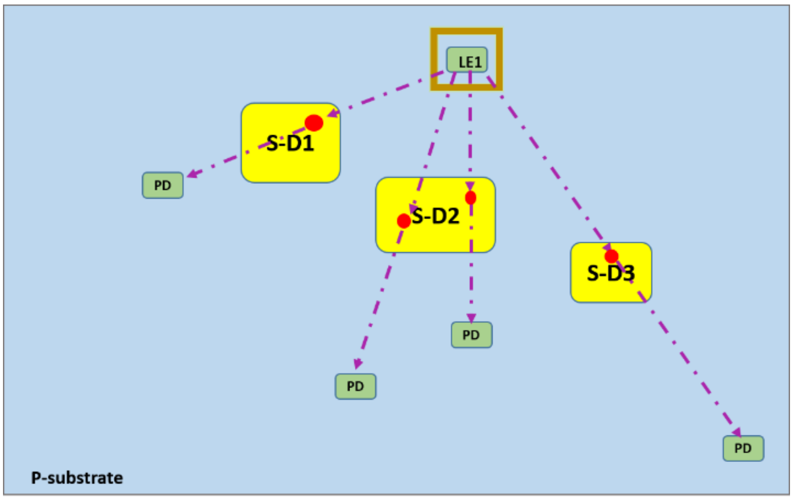


Fig 4. 17 Top view of the chip with one LE (light-emitting devices) and the allocated detectors at different intervals from the LE to protect the silicon backside underneath the security-sensitive devices (S-D).

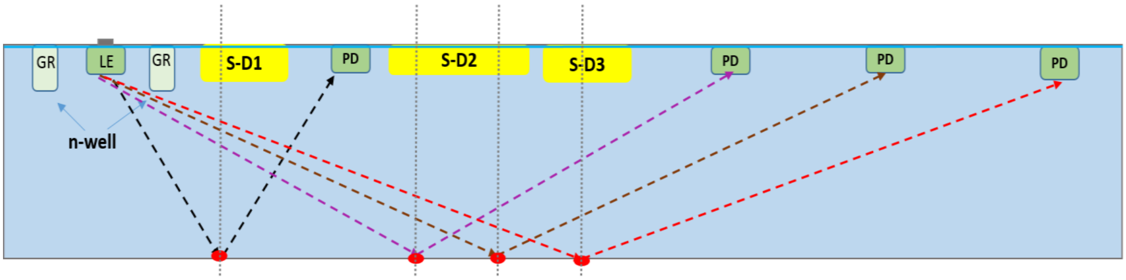


Fig 4. 18 Cross-section of the chip with one LE (light-emitting devices) and detectors located at different intervals to protect the silicon backside underneath of the security-sensitive device areas (S-D). GR is an n-well around the LE that acts as a guard ring.

The number of detectors for covering the area underneath each sensitive device depends on the size of the device as well as the size of the minimum area that is needed to be exposed to access to the secure data. For example, Tajik et al. [90] extracted the plaintext data from a common FPGA without any chip preparation and silicon thinning just by using the method of the contactless optical probing. In this chip, the whole logic area is about 200µm× 2mm, but the critical areas are small. They extracted the plaintext data from the AES (Advanced Encryption Standard) output port. It is shown in Fig 4.

19. In this case, it is necessary to allocate at least two detectors for these areas (one for (a) and one for (b)).

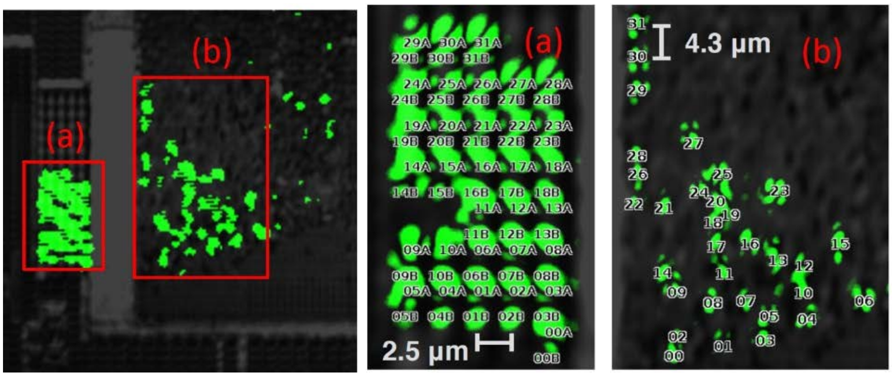


Fig 4. 19 Mapping of the plaintext bus bit locations for plaintext data extraction (a) AES output port, (b) logic meshes inside the AES [90].

There are probably several critical areas on the chip where attackers can extract the data which needs to be protected. The manufacturers and designers know all the critical and sensitive areas which are necessary to be protected. They are capable of designing the sensitive structures in a compact space and optimizing the number of required light emitters and detectors.

The area that each detector can cover is proportional to the size of the detector (surface of the drain). This proportional factor is one. So, according to the size of the detectors, one can determine how many detectors are required to protect each sensitive area.

The photocurrent of the detectors is directly proportional to the intensity of the incident light, and the intensity of the light is inversely proportional to the square of the distance from the light source. The radiant flux emission of a light-emitting device depends on the current flowing through it. Increasing the current will increase optical output power and luminosity of light [91]. Applying excessive forward voltage (forward current) to a p-n junction may cause severe degradation of the device performance. Therefore, applied current to the LE must be kept below the maximum ratings of the technology.

In case that chip is extensive, or the sensitive areas are far from each other, as well as the intensity of the electroluminescence of the LE is not sufficient to affect all detectors, it requires to allocate two or more light sources in order to check the integrity of the layer underneath all sensitive devices. Fig 4. 20 illustrates that LE1 and LE2 both are used as light-emitting devices. Some detectors may be affected by both LEs and some only by one LE. It should be mentioned that in this method, we can use as many detectors as required since the transistors are available all over the chip.

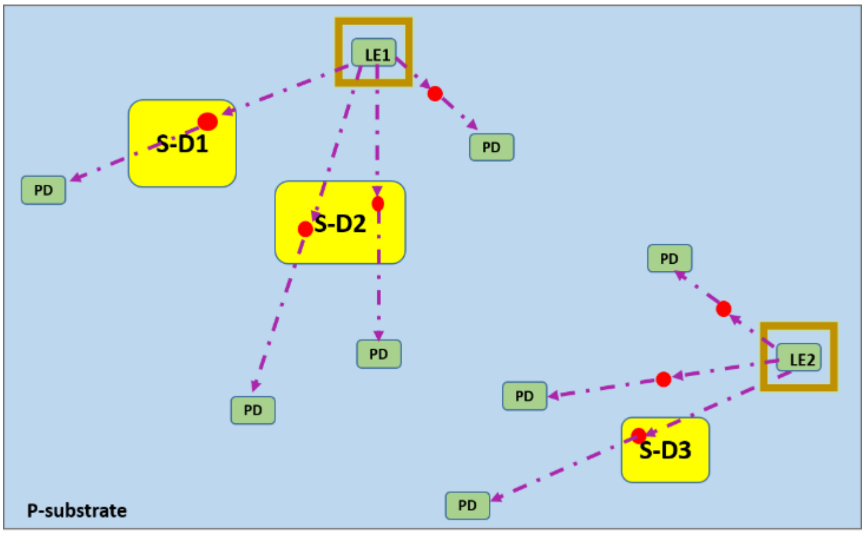


Fig 4. 20 Top-view of a large chip with two assigned light-emitting devices (LEs) and allocated detectors at different intervals to protect the silicon backside underneath the sensitive device areas (S-D).

4-4 Advantages and drawbacks of the protection mechanism

Using an optically active layer as a protection structure to defend the IC against attacks through silicon backside and checking the integrity of the layer optically by employing the IC components has many advantages:

(1) Optically monitoring the backside does not need an electrical connection between the frontside and the backside.

(2) This method employs the electronics of the IC to signal the violation of back-surface protection. These elements are generally available on the circuitry side of the IC; even if they do not exist, making them does not require an additional step for manufacturing.

(3) In consideration of contemporary technology, preparing the optical film is not expensive, and therefore, this technique is cost-effective. Furthermore, the coating process is done at room temperature, so the IC structures are not damaged by overheating.

(4) There are no restrictions on the IC application and packaging since only a thin layer is deposited on the IC backside, and there is no need to encapsulate the IC.

(5) There is no limitation for the silicon bulk, so the designer can utilize any thickness they want.

(6) Furthermore, the signal of the detectors, which is configured by the protection structure, can be used as an identifier or a secret key to encode sensitive data. In this case, accessing the data requires a flawless protection layer. If some random roughness is created on the IC back surface before coating the layer, the reflection varies from one device to another, and the ratio of the photocurrents in each IC would be unique so that the protection mechanism would be a physical unclonable function (PUF).

Although this method has many advantages, there is a drawback as well. In most ICs, silicon is the base material. Silicon has an indirect bandgap, and consequently, the electroluminescence intensity is low. Therefore, a silicon p-n junction should be operated in a high forward bias condition to emit light sufficiently [40]. Running the light emitter in high forward bias condition may result in the degradation of the devices. It may be advantageous to assign a particular light emission spot and conduct norming measurements from time to time as the source ages.

Replacing the silicon light source with a robust, non-silicon light source with light stability improves this protection mechanism. The best efficiency comes when a direct bandgap semiconductor is used as a base material for the light emitter.

In some modern technology like FinFET, there is plenty of germanium (Ge) in the active regions (junctions). Considering the spectral absorption coefficient of germanium and silicon presented in Fig 4. 21, a non-silicon LED that emits in the wavelength where silicon is transparent, and germanium is highly absorptive, such as at 1.3µm (1300nm) can be used. Therefore, germanium detectors will show a higher photocurrent even with a lower power on the LED. However, this is not the case for all semiconductor devices.

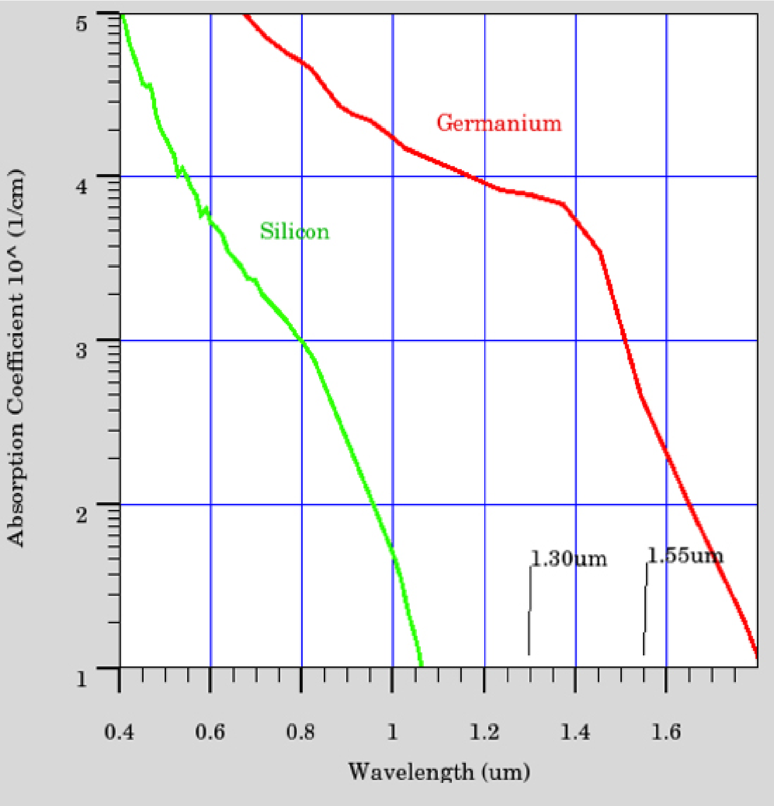


Fig 4. 21 Absorption coefficient of silicon and germanium [92].

In the next section, using of a non-silicon light emitter for this defense mechanism is considered.

4-5 External LED (Non-silicon light source)

In this section, alternatives for the light source which can be used for this method are discussed. Silicon is the base material for most of the ICs, and with today's technology, we cannot have a non-silicon diode within the IC. Therefore, an efficient light-emitting diode (LED) made of semiconductor material with a direct bandgap can be used as an external LED to create an optical signal.

An LED to be applicable for this technique must firstly emit light in the wavelength that is absorbable by the drain and the source of the transistors that are used as detectors. Second, it should emit in the direction where the photodetectors absorb only the light reflected on the IC backside. This means a proper placement of the LED onto the chip is necessary. Third, the optical power of the LED should be enough to affect the photodetectors.

In order to have an efficient LED, it is essential to define the wavelength where the detectors have the maximum absorption. It is also important to consider that light is partially absorbed by the silicon substrate as it passes through the bulk to reach the detector. In order to find this wavelength, the photocurrent of a detector over varying light wavelengths is measured. The detector used for this measurement was a p-n junction produced in 250nm technology with a doping concentration of about $10^{20}/cm^3$. For this assessment, light reaches the detector vertically from the backside of the IC, where the thickness of the IC (silicon bulk) is 310µm. A schematic of the measurement setup is shown in Fig 4. 22. The emission power was almost the same for all wavelengths. Thus, the photocurrent curve over the wavelength can be considered as a spectral response of the detector. The response curve is normalized from zero to one. In the spectrum shown in Fig 4. 23, the curve illustrates that the detector has its maximum absorption at the wavelength of 1010nm. This wavelength may differ slightly for different technologies and depends on the thickness of the IC. For each device to protect with this method, the thickness of the chip and the location of the detectors are already known. Therefore, one can easily calculate the light path length to get to the farthest detector. Fig 4. 24 shows the schematic cross-section of the LED and a photodetector, where d is the chip's thickness (silicon bulk depth), and X is the horizontal distance between LED and PD. X and d are known; thus, one can calculate the length of the path that the light should travel to get to the PD which is 2L (from LED to the back surface, and from the back surface to the PD).

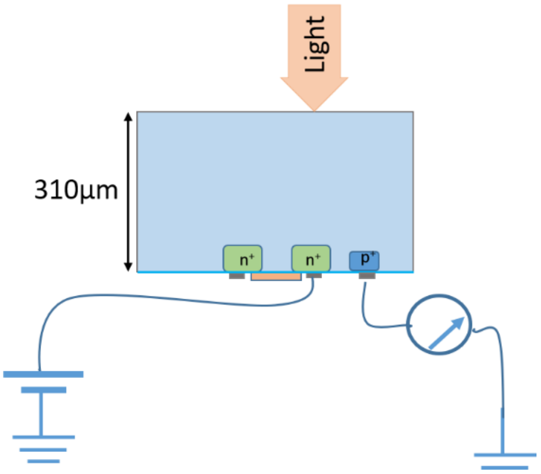


Fig 4. 22 Measuring the photocurrent of the detector when a light in the range of 800-1200nm hits the IC backside.

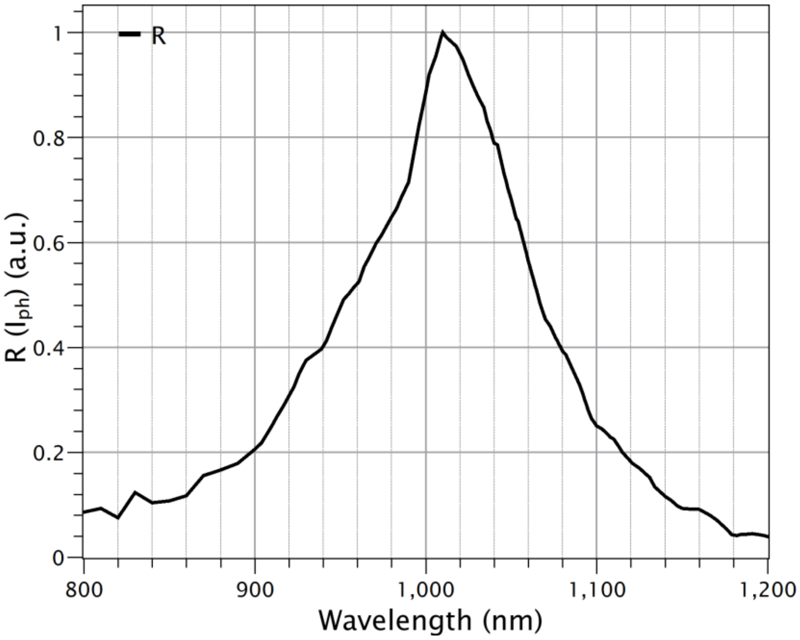


Fig 4. 23 Response of a detector (Photocurrent) to the light with different wavelengths. The detector is a p-n junction in a silicon IC with a thickness of 310µm. The light hits the detector from the IC backside.

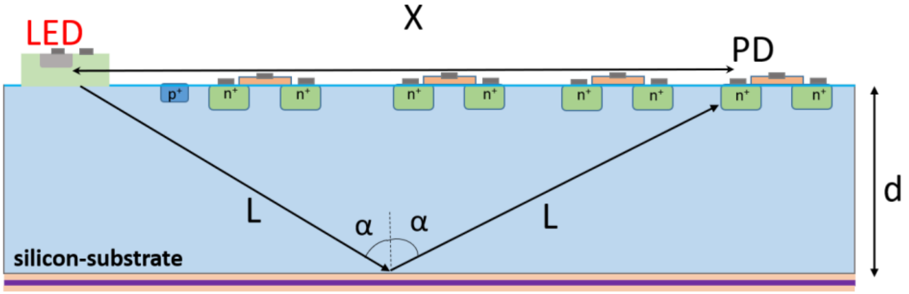


Fig 4. 24 Cross section of the chip where light emitter (LE) and detector (PD) are located. X is the lateral distance between LED and PD, d is the thickness of silicon, α is the angle of incidence, and L is the pathlength of the light before and after reflection.

The intensity of the light at each point in a medium can be calculated with the equation:

$$I(x) = I_0 e^{-ax} \tag{1}$$

where a is the absorption coefficient of silicon, x is the distance between the light source and the point at which the light intensity is being calculated, and I_0 is the intensity at the light source [93].

Since there is a direct proportion between the photocurrent and the light intensity, by applying equation (1) to the measured photocurrent, one can simulate the response of the detector when it absorbs a light with different path lengths in the silicon. The green, blue, orange, and pink lines in Fig 4. 25 demonstrate the calculated response (photocurrent) of the detector where the light travels through the silicon bulk in a depth of 300µm, 600µm, 900µm, and 1100µm, respectively.

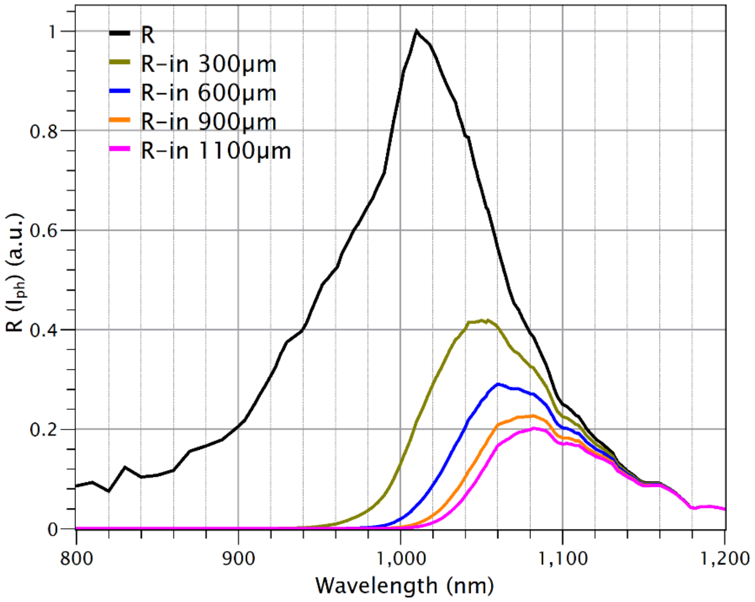


Fig 4. 25 The response of a detector (Photocurrent) over the wavelength to the light in different depths in silicon. The measured I_{ph} (R) where the light hits the PD after traveling 310µm in silicon bulk (black line) and the calculated R for PD in the more depth of 300µm-1100µm. The light hits the detector from the IC back-surface.

Comparing the curves explains that the wavelength of the maximum response has been shifted to a longer wavelength with the increasing depth of bulk. The photocurrent of the detector is reduced if the detector is placed at a greater distance from the light emitter. There are two reason for that. (1) photons with shorter wavelengths are absorbed by the silicon bulk more than photons with longer wavelengths. (2) The detector is a silicon p-n junction, and there is a low absorption coefficient for silicon at larger wavelengths. Thus, the light source must emit at a wavelength that all detectors respond to, and this wavelength is the peak of the response of the farthest detector. For instance, if 2L for the last detector is 1410µm (1100 +310µm), the illumination peak of the light emitter must be at 1070nm. Therefore, a narrow band emitting device is recommended because in wide-band emission, part of the radiation with higher energy (lower wavelength) will be absorbed by the silicon bulk, and the detector is not responsive to the light with lower energy. The emission spectra of the LED must be like the red curve in Fig 4. 26.

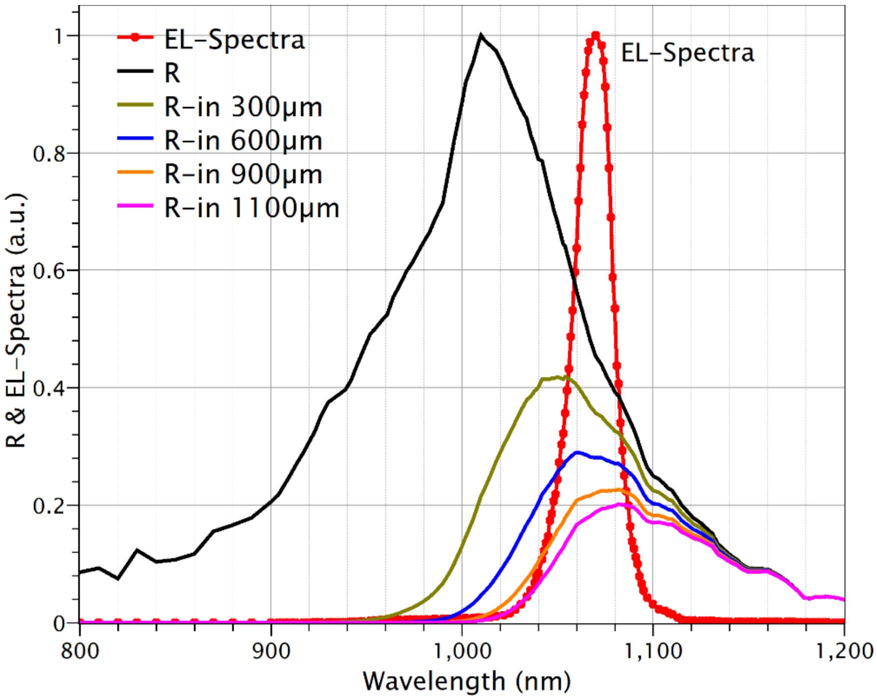


Fig 4. 26 The spectral response of a detector (photocurrent) at different depths in the silicon and the spectral emission of the external LED (red curve) applicable for emitting at a depth of 1410µm in the silicon.

In order to maximize the angle of the incidence of the LED light within the IC (silicon-substrate), the LED must be placed in contact with the IC, and the LED material should have a refractive index close to the silicon's refractive index. For instance, GaAs (Gallium Arsenide) can be an appropriate choice [94]. The refractive index of silicon at 1070nm is 3.55 [95], whereas GaAs has a refractive index of 3.45for the same wavelength [96].

Therefore, our non-silicon LED can be a single p-n junction formed by a layer of p-type doping in an n-type GaAs wafer. Besides material, the location of the external LED on the chip is an important consideration that is discussed in the following section.

4-5-1 Placement of the external LED into the chip

In each IC, the side where the IC components (transistors, capacitors, ...) are located is called the frontside. The backside refers to the back-silicon substrate side. On the frontside, on top of the active region, there are several layers of metal connections, interconnect wires, dielectrics, and meshes (as shown in Fig 4. 27).

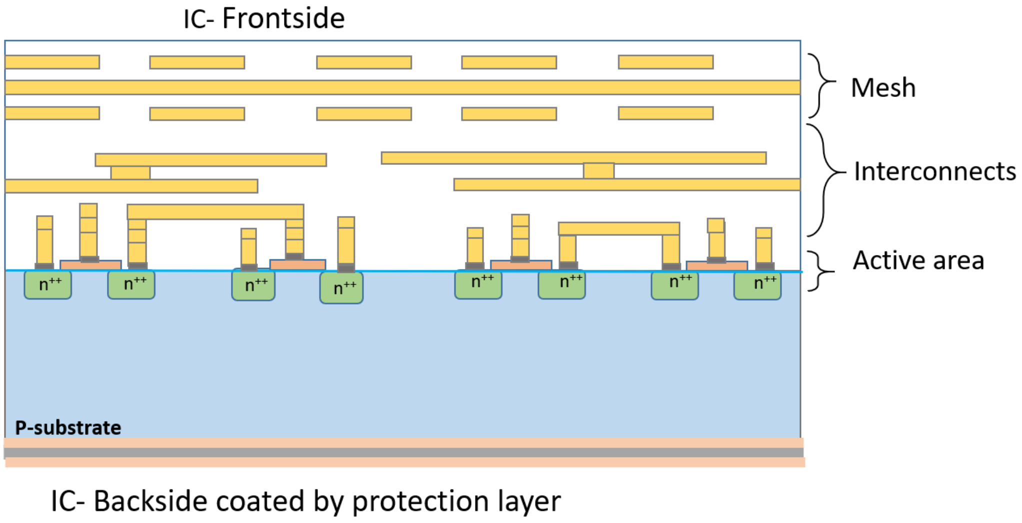


Fig 4. 27 Cross-section of the IC with interconnects and meshes on top of the active region. The backside is protected with an opaque layer.

In order to generate an optical signal inside the IC using an external LED, the LED should be placed in contact with the IC. In general, there are three ways to place the LED in contact with the IC, namely from the frontside, backside, or along the sides. If the LED is placed on the IC backside, as shown in Fig 4. 28 (a), light is unable to penetrate the opaque protection layer. It is not desired to place the LED after the layer on the silicon (Fig 4. 28 (b)) as well, because light will reach the detectors directly without interference.

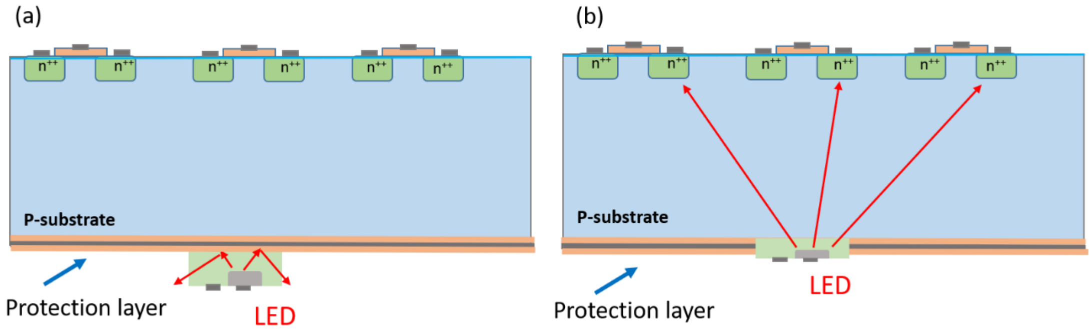


Fig 4. 28 IC cross-section. LED is placed on the IC backside of the IC, (a) before the protection layer, (b) after the protection layer.

In the case that the external LED is placed along the side of the IC, light enters the silicon in all directions, as shown in Fig 4. 29 (a), some towards the backside, which reflects on the coated silicon and some towards the IC components. Since the direct light path from the emitter to the detector is the shortest, the intensity of the reflected light from the coated layer is significantly lower and hence not desirable. One way to mitigate this is to coat an opaque layer on a portion of the LED surface to block the direct light path between the LED and detectors and direct the emanating light at a certain angle. Fig 4. 29 (b) illustrates this issue schematically. However, this is not a favorable location for the LED, especially for large-area devices such as FPGAs, where the circuits of high sensitivity are located further away from the sides.

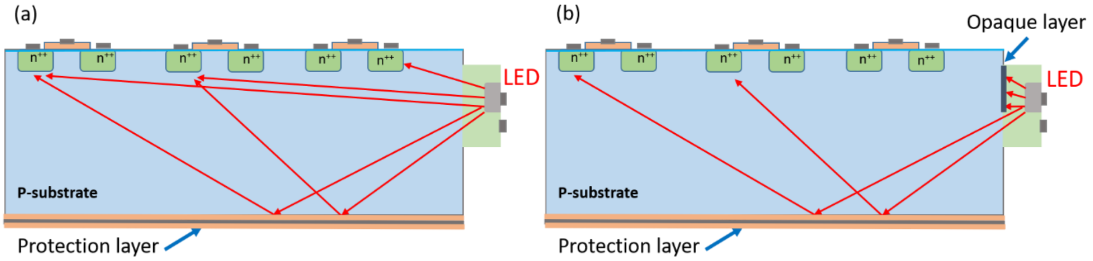


Fig 4. 29 IC cross-section. (a) LED is placed on the side of the IC; (b) an opaque layer is deposited on a portion of the LED surface to restrict the light, which goes directly to the detectors.

Similarly, the placement of the LED on the frontside of the IC (on top of the metallization and dielectric), or in between the interconnects, as shown in Fig 4. 30, of the IC is unable to achieve the desired outcome because of very limited light penetration through the dense metallization to enter the silicon and reach the reflective surface. The most efficient way to place the LED on the IC frontside is by removing the metal layers and dielectric from a small portion of the chip, within the area of interest. In this case, there will be little obstruction, and light will emit into the IC towards the IC backside, and the light reflected on the chip backside will be detectable by photodetectors, as shown in Fig 4. 31. Accordingly, the surface of the LED, which is in contact with the silicon, must be quite smooth. The p-n junction must be on top of the GaAs wafer so that light can pass through the GaAs and enter the silicon. As the absorption coefficient of the GaAs for wavelengths over 1000nm is insignificant and much lower than silicon, the light intensity reduction caused by GaAs is ignorable [94].

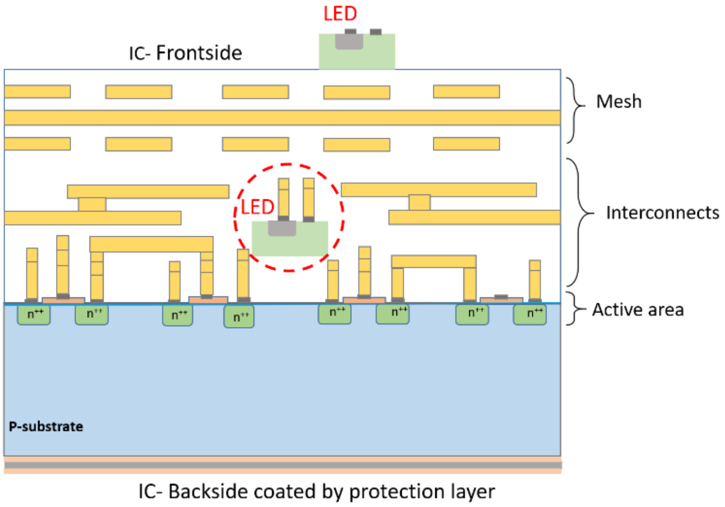


Fig 4. 30 IC cross-section. LED is placed on the frontside, on top of metallization, or between the metal layers of the IC.

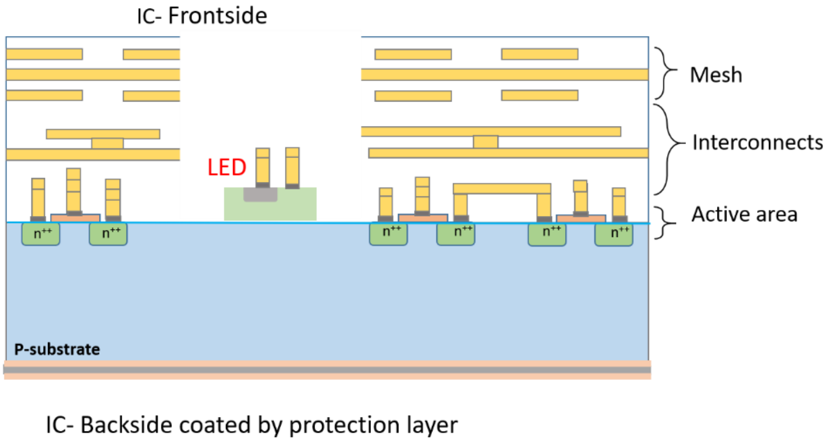


Fig 4. 31 IC cross-section. LED is placed on the frontside of the IC after removing the metal layer and dialectic.

The optimal way to generate an optical signal is to grow a non-silicon diode directly on a silicon substrate in the IC fabrication process steps. Although making a non-silicon nanowire laser on silicon is under research investigation, the practical applications of such kinds of devices are still in its early stages [97][98].

4-5-2 Advantages and drawbacks of the external LED

This section discusses the advantages and drawbacks of using a non-silicon LED for the IC protection mechanism and compares it to a silicon LED. First, the electroluminescence of the silicon LED and non-silicon LED are compared. Fig 4. 32 shows the spectral Si-LED emission and the spectral response of the photodetector. Comparing these two curves illustrates that most of the Si LED radiation is in the range where the detector is not responsive or has very low absorption. The maximum emission is at 1110nm while the maximum responsivity is at 1010nm when the light hits the PD's surface (PD is placed in a depth of 310µm in the silicon bulk), which shifts to 1070nm when light travels 1100µm more in the silicon, and then hits the PD (discussed earlier). The emission spectra of a non-silicon LED can be specified by optimizing device parameters. For instance, in this case, an LED emitting at 1070nm is needed. However, shifting emission spectra into the shorter wavelength leads to high absorption in the silicon bulk and decreases light intensity at the detectors. Hence, a trade-off must be made for the overall optimization. When the light travels into the silicon, its intensity decreases, and the intensity at each point can be calculated with equation (1). Fig 4. 33 compares the EL-spectra of the silicon and non-silicon LED at different depths in silicon (at LED, 600µm, and 1100µm).

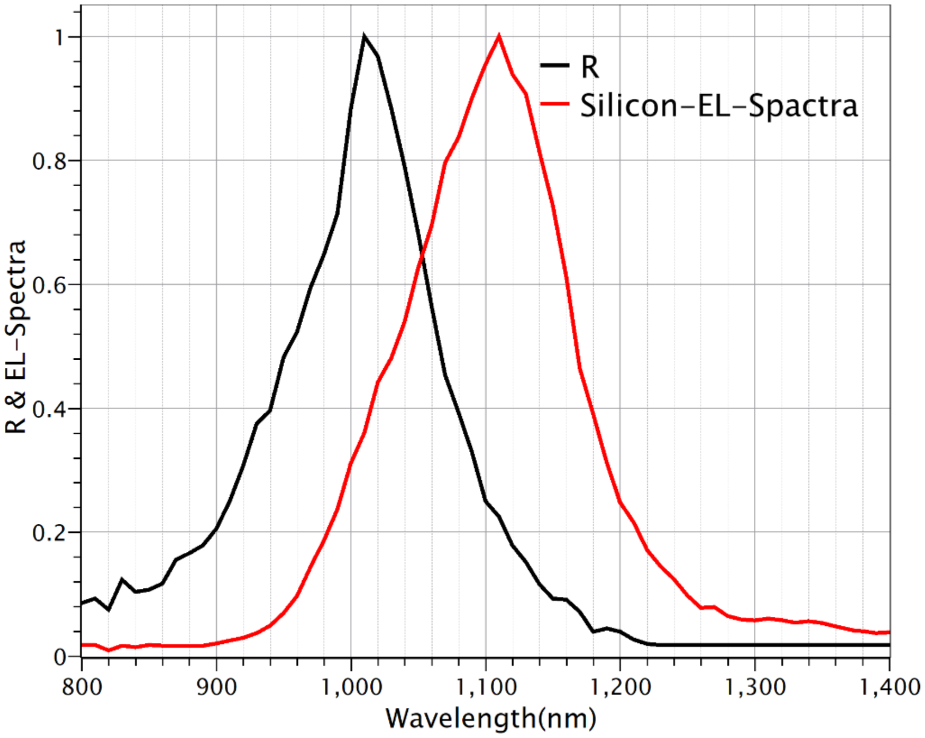


Fig 4. 32 Emission spectra of silicon LED (red line) and the response of the detector (black line).

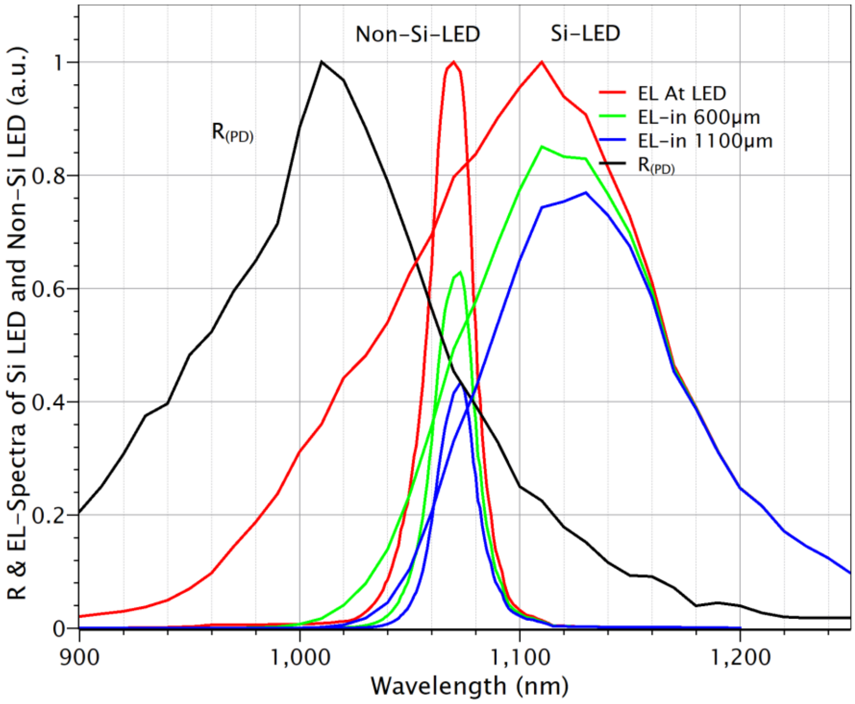


Fig 4. 33 Emission-Spectra (EL) of the Si LED, and non-Si LED at the different depths inside the silicon and response of detector (RPD).

Multiplying the emission spectra by the response of the detectors gives the portion of the emission that detectors respond to. This emission is calculated for the Si-LED and non-Si-LED at different depths and the values are compared in Table 4. 3. EL-I is the intensity of light at each point (integration of curves in Fig 4. 33). R(x) is the response of the detector to the incident light at each point ($R_{(PD)}$* EL-I $_{\text{(at each point)}}$) which gives the fraction of light intensity (at LED) that the detectors respond to. Results in Table 4. 3 show that in the best case where the Si-LED emission hits the surface and detector is exposed under the total emission, only 33.44% of the light will be absorbed by the detector, whereas this amount increases to 49.96% for a non-Si LED. However, the intensity of the light at longer distances is higher when a Si-LED is utilized, but the detector is more responsive to the non-Si-LED. The overall conclusion of Table 4. 3 is that the responsivity of the detector increases from 10.14%-33.4% for the Si LED to 16.82%- 49.96% for the non-Si LED for a light path length between 1100-0µm. Note that the numbers reported in Table 4. 3 are not the real responsivity of the detector, but the normalized data compares the behavior of the detector at different depths and its reaction to different LEDs.

Table 4. 3 Percentage of the emission-intensity (EL-I) of the Si LED, and non-Si LED and the response (R) of the detector at different points inside the silicon in ratio to the EL-I at the LED

Light path length between LED & PD	**Silicon-LED**		**EX-LED (non-Si)**	
	%EL-I	**%R(x)**	**%EL-I**	**%R(x)**
0μm	100	33.44	100	49.96
300μm	77.42	19.07	74.20	35.79
600μm	68.52	14.07	56.66	26.61
900μm	62.71	11.38	43.84	20.13
1100μm	59.70	10.14	37.16	16.82

The second and greatest advantage of a non-Si-LED over a Si-LED is that the non-Si-LED is made of a direct semiconductor. Radiative recombination is the process that dominates in the direct bandgap semiconductors, which is not the case for Si-LED but for GaAs-LED. This means the intensity of the produced light from a non-silicon LED is much higher that of a Si-LED when both are under the same input voltage. The third advantage of a non-Si-LED over a silicon one is that one can get rid of the destructive effect of using the silicon light emitter in high forward bias, such as device degradation.

Although using a non-Si-LED for the protection mechanism has many advantages, there are some drawbacks as well. For instance, adding an external LED into the chip will add an additional step in manufacturing and increase the costs. Another issue is the placement of the LED into the chip. Since the light must pass through a Si-GaAs interface to enter the silicon, the silicon and GaAs surfaces must be sufficiently smooth and should be in good contact with each other.

Chapter 5: Conclusion and future work

Modern integrated circuits (ICs) are at permanent risk of hardware attacks on sensitive data. So far, several countermeasures against such attacks have been introduced, but all such countermeasures can be circumvented by physical attacks through the unprotected silicon backside. This work has introduced, realized, and developed a cost-efficient countermeasure to defend the ICs against physical and optical attacks that target the IC through the chip backside. The presented protection mechanism consists of an optically active layer coated on the chip back surface along with the IC structures to generate and track the optical signal within the IC. The layer is opaque to the infrared light and provides angle-dependent reflectivity in the IR region. A regular p-n junction in forward bias operation is assigned to emit light towards the chip backside. The light emitter is designed and optimized to create an optical signal that is strong enough to travel inside the silicon and, after interaction with the layer on the backside, get reflected and be absorbed by the detectors at different intervals on the frontside. The light detectors are reverse-biased p-n junctions that are placed in various distances from the light emitter to absorb the optical signal reflected from the IC backside at a variety of angles of incidence. The absorbed light creates a photocurrent in the detectors. This photocurrent is directly proportional to the intensity of the light. Since the deposited protection layer on the chip backside changes the intensity of the incidence light depending on the angle of incidence of light, the photocurrent of detectors changes too. Therefore, the photocurrent of the detectors is specific to the deposited layer.

In this method, attack detection is performed by checking the integrity of the layer. A ratio of the photocurrent of the detectors is stored as a pattern in the device while the protection layer is intact. In order to check the integrity of the layer, the electrical signal of the detectors is measured and compared with the pattern. If the measured signal is not the same as the pattern, the device cannot confirm the integrity of the layer, then this is indicative of a backside attack. Subsequently, the device can be disabled, or sensitive data can be cleared away.

To determine the right material for the protection layer, a number of materials are investigated. The thickness and the condition of the process are optimized to achieve a layer with the desired properties. Accordingly, two optically active layers of ITO-Ag-

ITO and TiO_2-Ti-TiO_2 are designed and produced by the sputtering technique at room temperature.

In order to evaluate the protection mechanism in detecting an attack, the signals of the detectors are analyzed in the presence and absence of the protection layer. For this purpose, the two above mentioned layers are deposited separately on the backside of two different chips. Then the photocurrents of the detectors (the current created by the optical signal) after depositing and after removing the layer are measured and compared to each other.

The results of the electrical measurement indicate that the photocurrent of the detectors reduces after applying the protection layer, and the reductions depend on the AOI of light that is absorbed by each detector. The changes in the photocurrents are in good agreement with the changes in the reflectivity of the layer coated on the silicon backside. The results confirm that the optically active layer coated on the chip back surface specifies the photocurrents of the detectors, and any changes to the layer (that may result from tampering) cause changes in the photocurrents, which can be detected by the electrical measurements taken on the circuitry side of the IC. This protection structure has many advantages, which make it a very promising solution for securing the chip against attacks targeting the IC through the backside.

Through this work, some drawbacks have been identified, mostly around the light-emitting device. Some optimizations have been made, and a possible solution to improve the method has been discussed. For instance, some particular spots are assigned for light emission. To optimize the optical signal, a structure like an n-well, here called guard ring (GR), is placed around the light source. This guard ring partly restricts the direct light passage between the light-emitting and the light-sensing devices, as well as decreases the leakage current.

The position of the light emitter and the detectors are optimized depending on the size of the device, silicon bulk thickness, and the size of the area to be protected. The solutions to protect a very large device are also provided.

An LED made of direct semiconductor material is introduced as an efficient light source that must be externally implemented into the IC circuitry side. The parameters of the LED, such as the wavelength of the emission, size, and based material, have been determined.

This protection mechanism administrates the IC structures to generate and detect the optical signal within the IC and create a signal upon the violation of the IC back surface. These structures are already available on the circuitry side, and even if they do not exist (e.g., single p-n junction for emitting light), their production does not require additional steps during chip manufacturing. The only additional step in manufacturing is deposition of the protective layer on the IC backside, which is not expensive. The deposition of the optical layer does not require a high temperature; therefore, the layer can be deposited on the chip back surface at any step in the manufacturing process.

Overall, this countermeasure is recommended for protecting the IC backside, as it is cost-effective and capable of preventing both physical and optical attacks through chip back surface and can be used for all kinds of security-sensitive ICs.

Future work

As a continuation of this work, a test structure with different sizes of transistors and p-n junctions as detectors, and an optimized light source has been designed. This test structure is produced in 180nm technology and will be used to evaluate the protection mechanism for the case that the detectors are not the same structures. In this test structure, the drain and source of the general transistors of different sizes and single p-n junctions with different doping levels are employed as detectors.

Furthermore, a non-silicon LED has been designed and fabricated. The LED is based on GaAs that is a direct bandgap semiconductor. The LED is designed to emit light at a wavelength of 1070nm to which the silicon bulk is partly transparent to and which the IC structures can absorb. This LED will be installed on the IC frontside as an external light source.

An interesting development that can be made in this protection mechanism is to create random roughness on the silicon back surface before applying the protective layer. This creates a different reflection in each IC and the signal of detectors in each chip would be unique so that the protection mechanism would be a physical unclonable function (PUF). This technique is in development.

Appendix

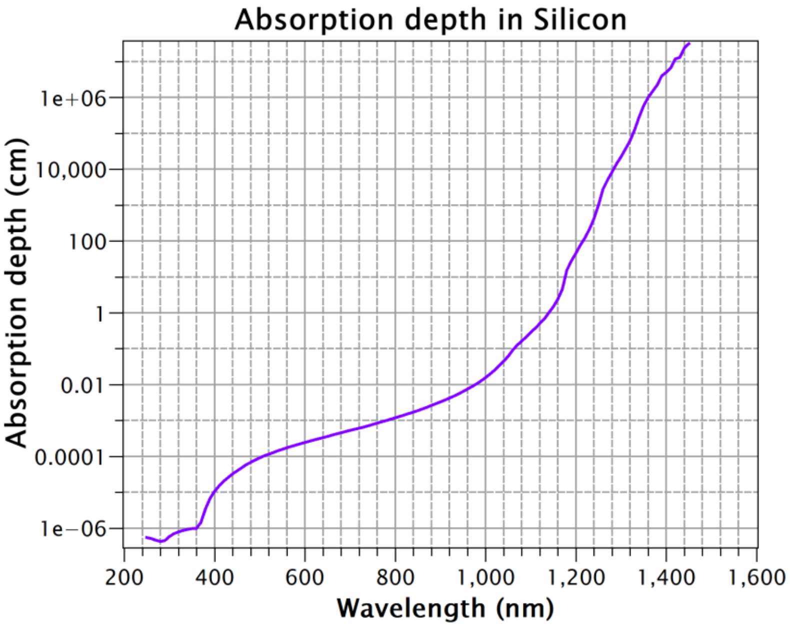


Fig 6. 1 Absorption depth in silicon [99]

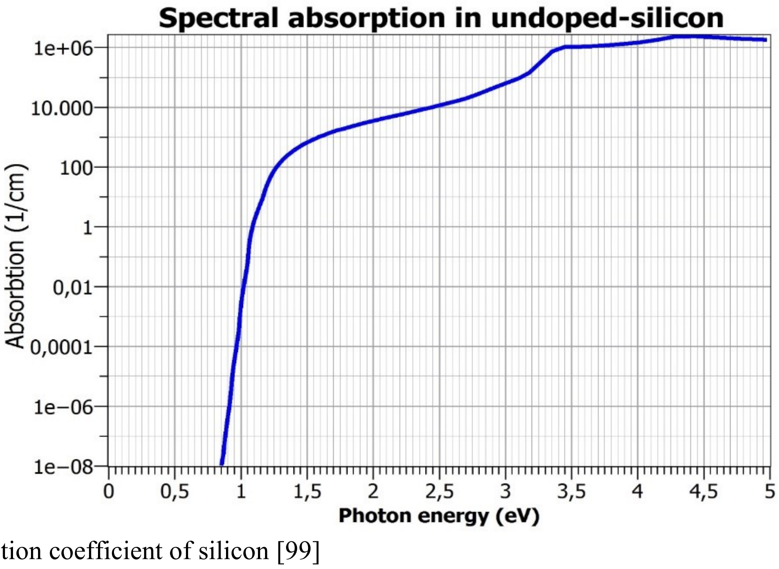


Fig 6. 2 Absorption coefficient of silicon [99]

References

[1] J.Villasenor, M.Tehranipoor: The Hidden Dangers of Chop-Shop Electronics: Clever counterfeiters sell old components as new threatening both military and commercial systems. IEEE Spectrum (2013).

[2] M.M. Tehranipoor, U. Guin, S. Bhunia: Invasion of the Hardwar Snatchers: Cloned Electronics Pollute the Market. IEEE Spectrum (2017).

[3] J. Villasenor and M. Tehranipoor "The Hidden Dangers of Chop-Shop Electronics: Clever counterfeiters sell old components as new, threatening both military and commercial systems"2013.

[4] M. Tehranipoor, C. Wang, "Introduction to Hardware Security and Trust", Springer Publishing Company, Incorporated, ISBN:978-1-4419-8079-3, 2012.

[5] K. Ahi, A. Rivera, A. Mazadi, and M. Anwar, "Fabrication of Robust Nano-Signatures for Identification of Authentic Electronic Components and Counterfeit Avoidance", Int. J. High Speed Electron. Syst., vol. 26, no. 3, p. 1740006, Sep. 2017.

[6] F. Koeune, F.X. Standaert, "A tutorial on physical security and side-channel attacks", in: Foundations of Security Analysis and Design III, 2005, pp. 78–108.

[7] K. Nohl, D. Evans, S. Starbug, and H. Plötz, "Reverse-engineering a cryptographic RFID tag". In Proceedings of the 17th conference on Security symposium (SS'08). USENIX Association, Berkeley, CA, USA, 185-193, 2008.

[8] S. Skorobogatov. "Hardware Security Evaluation of MAX 10 FPGA." ArXiv abs/1910.05086 (2019).

[9] S. Skorobogatov, "Semi-invasive attacks - A new approach to hardware security analysis", Technical report, University of Cambridge, Computer Laboratory, 2005.

[10] S. Skorobogatov and J. R. Anderson, "Optical Fault Induction Attacks". In Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), Burton S. Kaliski, Jr., Çetin Kaya Koç, and Christof Paar (Eds.). Springer-Verlag, London, UK, UK, 2-12, 2002.

[11] R. J. Anderson. 2008. Security Engineering: A Guide to Building Dependable Distributed Systems (2 ed.). Wiley Publishing.

[12] C. Helfmeier, D. Nedospasov, C.Tarnovsky, J. S. Krissler, C. Boit, and J-P. Seifert (2013). Breaking and entering through the silicon. Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 733–744.

[13] J. G. J. van Woudenberg, M. F. Witteman, and F. Menarini. 2011. Practical Optical Fault Injection on Secure Microcontrollers. In Proceedings of the 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC '11). IEEE Computer Society, Washington, DC, USA, 91-99. DOI: https://doi.org/10.1109/FDTC.2011.12.

[14] S. Tajik, H. Lohrke, F. Ganji, J-P. Seifert, and C. Boit. 2015. Laser Fault Attack on Physically Unclonable Functions. In Proceedings of the 2015 Workshop on Fault Diagnosis

and Tolerance in Cryptography (FDTC) (FDTC '15). IEEE Computer Society, Washington, DC, USA, 85-96. DOI=http://dx.doi.org/10.1109/FDTC.2015.19.

[15] F. Beaudoin, R. Desplats, P. Perdu, CNES; C. Boit, “Principles of Thermal Laser Stimulation Techniques”, Proceedings from the 43rd International symposium for testing and failure analysis (ISTFA 2004), Asm, PP.417-425.

[16] D. Samyde, S. Skorobogatov, R. Anderson and J. -. Quisquater, "On a new way to read data from memory," First International IEEE Security in Storage Workshop, 2002. Proceedings., Greenbelt, MD, USA, 2002, pp. 65-69. doi: 10.1109/SISW.2002.1183512

[17] S. Skorobogatov, “Optically Enhanced Position-Locked Power Analysis”. In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. Lecture Notes in Computer Science, vol 4249. Springer, 2006. doi.org/10.1007/11894063_6.

[18] H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, & J-P. Seifert, (2018). Key Extraction Using Thermal Laser Stimulation A Case Study on Xilinx Ultrascale FPGAs. IACR Trans. Cryptogr. Hardw. Embed. Syst., 2018, 573-595.

[19] D. Nedospasov, J. P. Seifert, C. Helfmeier and C. Boit, "Invasive PUF Analysis," Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on, Santa Barbara, CA, 2013, pp. 30-38.

[20] H. Lohrke, S. Tajik, C. Boit, and J.-P. Seifert. “No Place to Hide:Contactless Probing of Secret Data on FPGAs.” In: Cryptographic Hardware and Embedded Systems – CHES 2016. Springer, 2016, pp. 147–167. doi: 10 . 1007 / 978 - 3 - 662 - 53140 -2_8.

[21] J. Melngailis, “ocused ion beam technology and applications”, Journal of Vacuum Science & Technology B: Microelectronics Processing and Phenomena 5, 469 (1987); https://doi.org/10.1116/1.583937.

[22] C. A. Volkert and A. M. Minor. “Focused Ion Beam Microscopy and Micromachining”. MRS Bulletin 32 (05 2007), pp. 389–399. Issn: 1938-1425. doi:10.1557/mrs2007.62.

[23] A. Glowacki, C. Helfmeier, U. Kerst, and C. Boit. “Improvement of optical resolution through chip backside using FIB trenches”. In: Proceedings of the 36th International Symposium for Testing and Failure Analysis (ISTFA 2010). Vol. 36. ASM International, 2010, pp. 176–180.

[24] C.Rue, S.Herschbein, C.Scrudato, “Backside Circuit Edit on Full-Thickness Silicon Devices”. Proceedings from the 34th International symposium for testing and failure analysis, pp.141-150, Asm International, Nov 2008. DOI: 10.1361/cp2008istfa14.

[25] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J-P. Seifert (2013) Simple Photonic Emission analysis of AES. Journal of cryptographic engineering. 3. 10.1007/s13389-013-0053-7.

[26] D. Nedospasov, J-P. Seifert, A. Schlösser and S. Orlic, "Functional integrated circuit analysis," 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, San Francisco, CA, 2012, pp. 102-107. doi: 10.1109/HST.2012.6224328 .

[27] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks," in Proceedings of the IEEE, vol. 94, no. 2, pp. 370-382, Feb. 2006. doi:10.1109/JPROC.2005.86242.

[28] W. Rankl and W. Effing. 2010. Smart Card Handbook (4th ed.). Wiley Publishing.

[29] J.M. Cioranesco, J.L. Danger, T. Graba, S. Guilley, Y. Mathieu, D. Naccache, X.T. Ngo, “Cryptographically secure shields”, in: 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 25–31.

[30] S. Manich, M. S. Wamser and G. Sigl, "Detection of probing attempts in secure ICs," 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, San Francisco, CA, 2012, pp. 134-139. doi: 10.1109/HST.2012.6224333.

[31] M. Weiner, S. Manich, R. Rodríguez-Montañés and G. Sigl, "The Low Area Probing Detector as a Countermeasure Against Invasive Attacks," in IEEE Transactions on Very LargeScale Integration (VLSI) Systems, vol. 26, no. 2, pp. 392-403, Feb. 2018. doi: 10.1109/TVLSI.2017.2762630.

[32] S. Tajik, J. Fietkau, H. Lohrke, J. Seifert and C. Boit, "PUFMon: Security monitoring of FPGAs using physically unclonable functions," 2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS), Thessaloniki, 2017, pp. 186-191. doi: 10.1109/IOLTS.2017.8046216.

[33] Y. Gao, H. Ma, D. Abbott and S. F. Al-Sarawi, "PUF Sensor: Exploiting PUF Unreliability for Secure Wireless Sensing," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 64, no. 9, pp. 2532-2543, Sept. 2017. doi: 10.1109/TCSI.2017.2695228.

[34] S. Manich, D. Arumi, R. Rodriguez, J. Mujal, D. Hernandez, “Backside polishing detector: a new protection against backside attacks”, DCIS'15 - Conference on Design of Circuits and Integrated Systems. Estoril 2015, pp.1-6.

[35] H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, \Nanopyramid: An optical scrambler against backside probing attacks," in ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis. ASM International, 2018, p. 280.

[36] O. Kömmerling, F. Kömmerling (2006) Anti tamper encapsulation for an integrated circuit. US 7005733 B2.

[37] Zachariasse F (2012). patent US8198641 B2.

[38] https://semiengineering.com/whats-really-happening-inside-memory/

[39] https://en.wikipedia.org/wiki/P%E2%80%93n_junction#/media/File:Pn-junction-equilibrium.png

[40] B.E.A Saleh, M.C. Teic, “Fundamentals of Photonics,” John Wiley & Sons, 1991.

[41] W. Shockley, and W. T. Read, “Statistics of the Recombinations of Holes and Electrons”, Phys. Rev.87. p 835-842, 1952, (doi: 10.1103/PhysRev.87.835).

[42] R.N. Hall, “Electron-hole recombination in Germanium”, Phys. Rev 87, p387, 1952, (doi: 10.1103/PhysRev.87.387).

[43] S.M. Sze, Kwok K. Ng, “Physics of semiconductor devices”, J. Wiley and Sons, 1981.

[44] C.F. Lin, M.J. Chen, S.W. Chang, P.F. Chung, E.Z. Liang, T.W. Su and C.W. Liu, Electroluminescence at silicon bandgap energy from mechanically pressed indium–tin–oxide, Si contact, Applied Physics Letters 78, 1808 (2001).

[45] W. L. Ng, M. A. Lourenço, R. M. Gwilliam, S. Ledain, G. Shao & K. P. Homewood, "An efficient room-temperature silicon-based light-emitting diode"; Nature 410, 192-194 (8 March 2001).

[46] C. Boit, fundamentals of photon emission (PEM) in silicon electroluminescence for analysis of electronic circuit and device functuality, Microelectronics Failure Analysis (2004), pp. 356-368.

[47] S.E. Aw. H.S. Tan and C.K. Ong, "Optical Absorption Measurements of Band-Gap Shrinkage in Moderately and Heavily Doped silicon", J. Phys. Condens. Matter 3, 8213-8223 (1991).

[48] R.A. Falk, 2000. Near IR absorption in heavily doped silicon: An empirical approach. International Symposium for Testing and Failure Analysis.

[49] https://cleanroom.byu.edu/pn_junction

[50] www.sentech.com/en/SpectraRay-4-2309

[51] F.C. Chiu, T.-M. Pan, T.-K. Kundu, C.-H. Shih, "Thin film applications in advanced electron devices", Adv. Mater. Sci. Eng. 2014 (2014) 2, Article ID 927358.

[52] G. Catalan and J. F. Scott, "Physics and applications of bismuth ferrite," Advanced Materials, vol. 21, no. 24, pp. 2463–2485, 2009.

[53] P. C. Juan, Y. P. Hu, F. C. Chiu, and J. Y. M. Lee, "The charge trapping effect of metal-ferroelectric (PbZr0.53Ti0.47O3)(PbZr0.53Ti0.47O3)-insulator (HfO2)(HfO2)-silicon capacitors", Journal of Applied Physics, vol. 98, no. 4, Article ID 044103, 6 pages, 2005.

[54] B. Szyszka, "ITO Replacements: Insulator-Metal-Insulator Layers," In: Chen, J.; Cranton, W.; Fihn, M. (Eds.): Hndbook of Visual DisplayTechnologies, Springer, 2015, pp 819-832.

[55] F. Kastner, M. Bergsmann, H. Walter, G. Bauer; Method for producing tamper-proof identification elements. In: EP1558449B1, filed 2002.

[56] R.Wördenweber, "Deposition technologies, growth and properties of high-Tc films", Woodhead Publishing Series in Electronic and Optical Materials, 2011, Pages 3-37, 38e.

[57] J.E.ten Elshof, "Chemical solution deposition techniques for epitaxial growth of complex oxides", Woodhead Publishing Series in Electronic and Optical Materials, 2015, Pages 69-93.

[58] P.O'Brien, "Encyclopedia of Materials: Science and Technology (Second Edition)", Pages 1173-1176, 2001.

[59] J-O Carlsson, P.M. Martin, "Handbook of Deposition Technologies for Films and Coatings (Third Edition)", Pages 314-363, 2010.

[60] S. I. Shah, G. H.Jaffari, E. Yassitepe, B. Ali, "Evaporation: Processes, Bulk Microstructures, and Mechanical Properties", Handbook of Deposition Technologies for Films and Coatings (Third Edition), Science, Applications and Technology, Pages 135-252, 2010.

[61] A. Mubarak, E. Hamzah, M.R.M Toff, "Review of physical vapour deposition (PVD) techniques hard coating", Jurnal Mekanikal, 20, pages: 42-51, 2005.

[62] R. Herrmann, G. and Bräuer, "DC and RF-Magnetron sputtering", Handbook of optical properties, Vol. 1: Thin films for optical coatings. Hummel, R. E.; Guenter, K. H. (Eds.), CRC Press, 1995, p. 135-87.

[63] G. Bräuer, B. Szyszka, M. Vergöhl, R. Bandorf, "Magnetron sputtering - milestones of 30 years", In: Vacuum 84 (2010), S. 1354-9.

[64] M. M. Hassan, "Handbook of Antimicrobial Coatings", Elsevier, Pages 321-355, 2018.

[65] http://www.semicore.com/what-is-sputtering

[66] H. Adachi,T. Hata, K. Wasa, "Handbook of Sputtering Technology", Elsevier, Page: 295-359, 2012. DOI10.1016/b978-1-4377-3483-6.00005-x.

[67] P.J Kelly, R.D Arnell, "Magnetron sputtering: a review of recent developments and applications", Vacuum, vol. 56, issue 3, pp. 159-172, 2000.

[68] H.G. Tompkins, E.A. Irene (Eds.), Handbook of Ellipsometry, William Andrew Publishing, Norwich NY, 2005.

[69] H. Fujiwara, Spectroscopic Ellipsometry Principles and Applications, John Wiley & Sons Ltd, West Sussex, England, 2007.

[70] A. A. Khosroabadi and R. A. Norwood, "Spectroscopic Ellipsometry Study of Novel Nanostructured Transparent Conducting Oxide Structures," Proceedings of SPIE - The International Society for Optical Engineering; volume 8632 (2013).

[71] S. Skorobogatov, "Hardware Assurance and its Importance to National Security," 2012. [Online]. Available at: http://www.cl.cam.ac. uk / sps32 / secnews.html.

[72] A. Ryer, Light Measurement Handbook, ©1997-1998, URL: http://www.intl-light.com/handbook

[73] J.N. Hilfiker and R.A. Synowicki, J.A. Woollam Company, Lincoln, NE; and H.G. Tompkins, Consultant, Chandler, AZ5, "Spectroscopic Ellipsometry Methods for Thin Absorbing Coatings", 51st Annual Technical Conference Proceedings, Chicago, IL, April 19–24, 2008 ISSN 0737-5921.

[74] www.sentech.com/en/SpectraRay-4-2309

[75] https://www.sentech.com/en/SENpro__311/

[76] P.A.van Vijnatten, J.M.C. de Wolf, I.J.E. Schoofs; Spectrophotometer accessories for thin film characterisation, in: 7th ICCG (International Conference on Coating on Glass & Plastics), Breda, Netherlands, 2008.

[77] https://www.perkinelmer.com/de/product/lambda-950-uv-vis-nir-spectrophotometer-l950

[78] https://www.omtsolutions.com/products/absolute-reflectance-transmittance-analyzer-arta/

[79] A. Klöppel, W. Kriegseis, B.K. Meyer, A. Scharmann, C. Daube, J. Stollenwerk, J. Trube; Dependence of the electrical and optical behaviour of ITO-silver-ITO multilayers on the silver properties. In: Thin Solid Films 365 (2000), p. 139-46.

[80] E. Amini, R. Muydinov, B. Szyszka, and C. Boit, (2017) Backside protection structure for security sensitive ICs. Proceedings from the 43rd International symposium for testing and failure analysis, pp.279-284, Asm.

[81] E. Amini, A. Beyreuther, N. Herfurth, A. Steigert, R. Muydinov, B. Szyszka, and C. Boit, (2018) IC security and quality improvement by protection of chip backside against hardware attacks. Microelectronics Reliability 88-90C, pp. 22-25.

[82] E. Amini, A. Beyreuther, N. Herfurth, A. Steigert, B. Szyszka, C. Boit. "Assessment of a Chip Backside Protection. Journal of Hardware and Systems Security" (2018) 2:345–352.

[83] E. Amini, N. Herfurth, A. Beyreuther, J-P. Seifert, and C. Boit, "Generation and Tracking of Optical Signals inside the IC to Improve Device Security and Failure Analysis" 26th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), 2019. 10.1109/IPFA47161.2019.8984916.

[84] C. Boit, S. Tajik, P. Scholz, E. Amini, A. Beyreuther, H. Lohrke, J-P. Seifert, "From IC debug to hardware security risk: The power of backside access and optical interaction," 2016 IEEE 23rd International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), Singapore, 2016, pp. 365-369. doi: 10.1109/IPFA.2016.7564318.

[85] https://www.panacol.com/products/adhesive/vitralit

[86] F.Krannig, "chemical etching of ITO coatings", Applied Films Corporation, Boulder,CO.

[87] https://cdn-reichelt.de/documents/datenblatt/C900/DE_RE966-01E.pdf

[88] https://www.panacol.de/panacol/datenblaetter/structalit/structalit-5893-deutsch-tds panacol-kleber.pdf

[89] https://www.panacol.de/panacol/datenblaetter/structalit/structalit-5891-deutsch-tds panacol-kleber.pdf

[90] S. Tajik, H. Lohrke, J-P. Seifert, and C. Boit (2017) "On the power of optical contactless probing: attacking bitstream encryption of FPGAs". In proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS 2017).

[91] Taylor A.E.F (2000) Illumination fundamentals, Rensselaer polytechnic institute.

[92] https://www.silvaco.com/tech_lib_TCAD/simulationstandard/2010/apr_may_jun/a1/a1.html

[93] E. Hecht, "Optics" Reading, Mass:Addison-Wesley, 2002.

[94] W. G. Spitzer, and J. M. Whelan, "Infrared Absorption and Electron Effective Mass in n-Type Gallium Arsenide" Phys. Rev. 114, 1 (1959) 59-63.

[95] https://refractiveindex.info/?shelf=main&book=Si&page=Schinke

[96] https://refractiveindex.info/?shelf=main&book=GaAs&page=Rakic

[97] H.Kim, W.J. Lee, A.C. Farrell, J.S.D. Morales, P. Senanayake, S.V. Prikhodko, T.J. Ochalski, D.L.Huffaker.," Monolithic InGaAs Nanowire Array Lasers on Silicon-on-Insulator Operating at Room Temperature," Nano Letters 2017 17 (6), 3465-3470, DOI: 10.1021/acs.nanolett.7b00384.

[98] I. Giuntoni, L. Geelhaar, J. Bruns, and H. Riechert, "Light coupling between vertical III-As nanowires and planar Si photonic waveguides for the monolithic integration of active optoelectronic devices on a Si platform," Opt. Express 24, 18417-18427 (2016).

[99] M. A. Green, "Self-consistent optical parameters of intrinsic silicon at 300 K including temperature coefficients", Solar Energy Materials and Solar Cells, vol. 92, pp. 1305–1310, 2008.