Analysis of the problem of selling Recycled ICs and ways to detect if the chip under test is recycled.

I. Introduction

An integrated circuit is a collection of electronic circuits on a single, compact flat piece of semiconductor material, often silicon. It is also known as an IC, a chip, or a microchip. The chip has a significant number of integrated tiny transistors and other electronic parts. This produces circuits that are orders of magnitude quicker, cheaper, and smaller than those made of discrete components, enabling a high transistor density. Rapid adoption of standardized ICs in substitution of designs employing discrete transistors has been made possible by the IC's mass manufacturing capacity, dependability, and building-block approach to integrated circuit design. Integral circuits (ICs), which are used in nearly all modern electronic devices, have fundamentally altered the electronics sector. Modern computer processors and microcontrollers, which are small and inexpensive, have made it possible for computers, smartphones, and other home appliances to play a crucial role in the construction of contemporary civilizations. Very-large-scale integration has been made possible by technological advancements in semiconductor device manufacture. An region the size of a human fingernail may contain billions of transistors on a contemporary chip. Chips have drastically improved in size, speed, and capacity since they were initially created in the 1960s. This progress has been made possible by technological advancements that allow more and more transistors to fit on chips of the same size. Compared to discrete circuits, ICs offer three key advantages: size, cost, and performance. Because the chips are manufactured as a whole using photolithography rather than being built one transistor at a time, the size and cost are small. In addition, packed integrated circuits utilize a lot less material than discrete circuits. The IC's components switch rapidly and require very little power due to their compact size and close closeness, which boosts performance.

II. Consequences

As the integrated circuit (IC) production gets more globalized and complicated more sources of error are a concern. Particularly, it is much more difficult to assess the trustworthiness of IC suppliers, casting doubt on the offered parts. The ICs being sold by questionable sellers might have been purposefully renamed, illegally copied, or recycled from old or flawed circuit boards. Even if they initially work, these might have briefer lifetimes and provide dependability issues. The consequences can be catastrophic if important systems start to malfunction due to use of fake parts.

The reliability issues of a chip can be external as well as internal of course. Extrinsic problems occur over the course of the device's lifetime and can be brought on by things like process variation, flaws that surface during production, or flaws that are missed during testing. Intrinsic failures, on the other hand, occur during the manufacturing process and can be caused by flaws in the design of the chip under test. Even after being in operation for some time, a device may still experience reliability problems that need to be fixed. An IC, for instance, could have a predicted lifetime when it is supplied to customers, but when the reliability problems are resolved, it can survive a very long period.

Counterfeiting of integrated circuits has become a severe problem due to flaws in the current test solutions and a lack of efficient avoidance procedures in place. Governments and businesses are very concerned about them due to the potential harm they can do to jobs, economic growth, and innovation, the risk they pose to consumer welfare, the sizeable amounts of money they involve flowing to criminal organizations, organized crime, and other organizations that destabilize and pollute society, as well as the decreased revenues from the sale of counterfeit goods.

Concerning the financial ramifications counterfeit ICs make consumers less confident in the goods they buy. In addition to undermining genuine enterprises' ability to compete and depriving governments of tax income, the black market for counterfeit ICs also harms the economy.

Additionally, counterfeit ICs are frequently built with inferior materials and using production techniques that do not adhere to industry requirements. They thus have a substantially higher chance of failing, which might result mission failures, health issues, or safety dangers. For instance, in aviation, using fake ICs in flight control systems might have disastrous effects.

As we know innovation in the business sector, which takes the shape of the development and implementation of fresh concepts for goods and operations, has traditionally been the main driver of economic growth. These inventions are often protected by patents, copyrights, and trademarks. However, if these intellectual

property (IP) rights were not adequately protected, there would be far less motivation to produce these novel ideas and goods, which would downgrade innovation and critical thinking. In sectors where the cost of R&D to develop new items is significant relative to the cost of producing the finished goods, these risks are particularly serious.

Also due to the enormous rise in complexity of the ICs used in electronic systems over the past few decades, they are produced abroad to lower production costs. For instance, big foundries in several nations may offer design houses reduced pricing. As a result of globalization, there is now a covert market for parts that will undercut the competitors. So we can realize that If these components are used in vital systems like those for military, aerospace, or health, the outcomes might be fatal.

Additionally, it is estimated that $100 billion in annual global income is lost by legal electronics companies due to counterfeiting. The high-tech industry is, in fact, significantly impacted by counterfeiting activity. Around one percent of semiconductor, sales are thought to be counterfeit.

III. Counterfeit Types

We can categorize these counterfeit components into seven different groups.

1) **Recycled**: The kind that now attract the most attention are the ones that have been repurposed and identified as fakes. According to studies, the supply chain for counterfeit parts already in use today recycles more than 80% of them.
2) **Remarked**: Counterfeiters remove the existing marking off the box or even the die and replace it with new, fictional markings as they remark.
3) **Overproduced**: Currently, most high-density integrated circuits are made in modern industrial sites. It is said that the cost of building or sustaining such facilities with the current CMOS technology surpass several billion dollars and is rising. Over the last twenty years, the semiconductor industry has largely switched to a contract foundry business model as a result of rising costs and expanding complexity of foundries and their operations (horizontal business model).
4) **Out-of-Spec/Defective**: These parts may be being sold on purpose or they may have been stolen and sold on open markets.
5) **Cloned**: Many competitors and counterfeiters regularly perform cloning to copy a design and reduce the high development costs of a component.
6) **Forged Documentation**: The modification history of a component or certifications of compliance with certain standards or programs are examples of fabricated documentation. It may be difficult challenging to prove their legality

since the OCM may not have preserved documentation for older designs and parts.

7) **Tampered**: During every stage of a component's life cycle, changes can be made. Either at the die or the package level might be where the "hardware Trojan" resides. These parts can act as a backdoor, allowing an attacker to access sensitive data from the chip changing how the device behaves under specific conditions.

Since the counterfeit types consist 80% of recycled parts our focus is the recycled ones. When we refer to counterfeit chips we mainly speaking about the recycled.

IV. Counterfeit Defects

The detection of counterfeit components is challenging. The results of the detection are affected by different component kinds (analog, digital, etc.) and fakes. The detection of some fakes and the testing of particular components are easier than others. Finding one or more defects will enable one to clearly distinguish bogus components. The leads or packaging of a counterfeit item can be irregular, it might perform poorly, or it might have a different specification. Assuming that the components are fully tested during assembly, any abnormalities or incorrect behavior by them may be traced to being fakes.

1) Physical defects: The components' physical attributes and physical defects have a strong correlation. They may fall under the interior or exterior fault categories, depending on where they exist. how it relates to the packaging. The component package, leads, balls, and columns are the main causes of exterior faults, as well as shipping and packing. The packing or shipping that the parts arrived in will have flaws, and these will be the most obvious. If an IC has previously been used, the component's leads, balls, and columns can show how it was handled. The datasheet specifications, especially those of size and shape, should be physically followed by them. Leads should be finished with a coating that conforms with the specification sheet. The container of an IC could carry crucial information about the chip. Since all model numbers, country of origin, date codes, and other details are etched here, counterfeiters will take great precautions to prevent damage and keep the package appearing as authentic as they can. Bond wire faults and flaws associated with dies are the two basic types of interior flaws. Die connection difficulties, missing or damaged bond wires inside the package, etc. are common causes of bond wire troubles. The component's die provides a

significant amount of helpful information. This category includes die marks, cracks, and other flaws.

Electrical Defects: Typical electrical failures can be categorized into two categories: manufacturing problems and parametric defects. Parametric faults are changes in component properties brought on by prior usage or temperature. A chip's specifications will vary as it ages after being used in the field for a while. Process, material, and packaging faults are the three categories used to classify manufacturing problems. They are a byproduct of the component manufacturing process. The defects indicated under the process category are caused by the photolithography and etching techniques employed in the fabrication. Impurities present in the silicon or oxide layers are the root cause of material defects. The passivation layer offers some protection for the die, but failure occurs when corrosion causes pinholes or fractures. The aluminum layer is quickly contaminated in the presence of salt and chloride, which results in a resistive open defect.

V. Counterfeit Detection Methods

These are several detection methods for examining counterfeit parts that Manufacturers, distributors, and end users can use to identify the unapproved by OCM chip under test.

1) **Physical Inspections**: The initial set of tests performed on the arriving components for verification is frequently physical inspections. These are fixed on the leads, packages, and dies of the component components' physical properties.
    - **Incoming Inspection**: After being received, an order first passes through the arriving inspection. There are typically two methods to examining CUTs. Low power visual inspection, or LPVI, is usually the first test carried out to each component. The leads and packages are carefully investigated using a low-power microscope or magnification lamp. Part number, lot, date, country code, and other relevant information are all recorded, along with packing and shipping information. Recycled components can have apparent desoldered leads and extra material on them. Rarely, the older marking can still be seen underneath the new one. Scratches on the box are usually visible as evidence of recycling. X-ray imaging is an additional test. You may examine the interior of the component using X-ray imaging without removing its covering. Normally,

it is regarded to be a nondestructive test. The two main types of X-ray imaging systems are film and real-time X-ray systems. Real-time X-ray systems, contrary to film X-ray systems, which produce pictures on radiographic film, create a digital image utilizing digital sensors Anomalies and faults in the die and bond wire, such as incorrect or missing die, die fractures, broken bond wires, etc., might be found. To ensure that a component is legitimate, additional testing may be required. The use of X-ray imaging is a crucial technique for identifying fakes. To ensure that a component's internal package, match those of a legit part, certain procedures are followed. If the authenticated component cannot be accessed, comparisons should be done between items from the same lot.

- **Exterior Test**: The exterior section of the package are being inspected using external testing. In package configuration and dimension analysis, the CUTs' dimensions are measured with the use of a manual or automated equipment. A CUT may be a fake if there is any abnormal measurement mismatch from the specification sheet. Blacktop Testing involves using various solvents to see how long a CUT's marking will last. Microblasting analysis, a dry blasting technique, is used by counterfeiters to remove component markings and scratches from counterfeit parts and to falsely represent fresh parts (e.g., upgrading temperature or speed-grade by erasing part markings before Counterfeit Electronic remarking devices). Another method that is advised for hermetically sealed products is hermiticity testing, a type of package examination that confirms the hermetic seal. Such components' seals make ensuring they operate in the environment as intended. If this seal breaks, the component will stop functioning. A helpful technique for safely evaluating a component's structure is scanning acoustic microscopy (SAM). Using ultrasonic wave reflection and transmission, this method creates an image of the component based on the component's acoustic impedance at various depths. Given that air has a far lower acoustic impedance than any of the part's media, the area will seem notably darker in the image. The resolution of SAM is calculated using the transducer frequencies. At lower frequencies, poorer spatial resolution is obtained at the tradeoff of increased component penetration. SAM should be used to check for delamination or die adherence to the packaging. Additionally, it can find flaws in the die as well as holes, fractures, and anomalies in the bond wires.
- **Interior Test:** The die and bond wires are among the intrinsic CUT parts that need to be investigated via decapsulation. There are three

decapsulation methods are often utilized. These methods are mechanical, chemical, or laser-based. When the component has been decapsulated and the essential structures have been identified, the following tests must be performed:

Optical examination thoroughly records all pertinent information about interior of the chip. Bond wire locations, bond kinds, and other relevant details must all be recorded. Die markings including manufacturer's nation, chip ID, date code, and corporate logo, must also be recorded. To evaluate how well the links with the die are made, a wire pull is utilized. The bond wires and die gradually lose their adhesion to one another over time when the chip is in use. By comparing the pull (pulling force) with a legit chip one may determine whether or not anything has been previously utilized. Throughout die shearing, the integrity of the die attach is inspected and only hermitic components pass this test. A ball shear test is used to examine the consistency of the ball bond at the die. A focused electron beam is used in Scanning Electron Microscopy (SEM) to produce pictures with incredibly high resolution. The image is shown on the control panel while the column produces a concentrated electron beam to scan the surface Backscattered electrons and X-rays are emitted as a secondary emission as a result of the high energy electron beam's interaction with the material. These secondary electrons are found by an electron detector, which then creates a picture. SEM is an effective method for finding various flaws and oddities in counterfeit chips.

- **Material Analysis**: Material analysis is used to confirm the CUT's chemical make-up. These are the only methods that are capable of identifying material-related flaws and irregularities. The use of inferior materials, contamination, lead oxidation, and other problems might all be considered defects. There are many tests available to evaluate the materials. X-Ray fluorescence spectroscopy (XRF) is a non-destructive method for material examination. After a vigorous high-energy X-ray bombardment, a material's emission properties are examined. When an X-ray hits a material's surface, the outermost electrons have enough energy to enter unstable higher outer orbits. When these electrons return to their initial ground state, radiation is emitted. Each element creates its own peak in the spectrum. Using XRF spectroscopy, a fingerprint specific to a component may be created from its packaging. Comparing a product to an authenticated sample or the manufacturer's datasheet can be used to determine its legitimacy. It is possible to analyze materials using a variety of X-ray fluorescence spectrometers. The Fourier Transform Infrared Spectroscopy (FTIR) test is another one

that uses IR spectroscopy to operate. While some of the IR radiation is absorbed by the item under test, some of it is transferred. Infrared light, which is created by the process, displays the spectrum of molecule absorption and transmission. The specific molecular fingerprint generated by FTIR is contrasted with legit's fingerprint to provide a comparison of materials. FTIR It is used to look at the polymer, coating, and other parts of the package as well as any foreign materials left over after the sandblasting process. Energy-Dispersive X-ray spectroscopy (EDS) is used to chemically characterize a component using X-ray excitation. A high-energy river of charged molecules strikes the surface, and the X-ray spectrum that is released is captured by an X-ray detector to produce the EDS spectrum. The packing materials for the component leave a specific X-ray spectral fingerprint.

2) **Electrical Inspections**: These checks are when counterfeit components are typically found to have electrical faults and abnormalities. For these examinations, four categories have been established.
    - **Parametric Tests**: Parametric testing is a test that measures a component's parameters. The DC and AC values may not match the given value if the chip has already been utilized. The results of a parametric test can be used to assess if a chip is real or not. During DC parametric testing, an ATE's measuring unit drives an I/O voltage and current to a steady state before applying Ohm's law to measure the electrical properties. The DC parametric tests may be divided into a variety of categories, such as contact tests, power consumption tests, output short current tests, output drives current testing, threshold tests, etc. Tests using AC voltages at a certain frequencies are used to evaluate AC parameters (such as terminal impedance, timing, etc.). AC parametric testing may be divided into the following categories: tests for propagation delays, tests for setup, hold, and release times, etc. Examples of DC parametric tests include leakage testing. Examples of AC parametric tests include setup time sensitivity testing, access time tests, running time tests, etc.
    - **Functional Tests**: Functional tests are the most efficient technique to ensure a component's functionality. Most of the issues may be found by these tests. Any imperfection that impairs performance can be identified, from little ones like broken or missing bond wires to more serious ones like problems in the manufacturing process. A component's functioning is assessed during function verification. It examines if several parts, which can have been created using various technologies, can work together as a system and deliver the desired result. Also Read/write

operations are carried out on memory during memory testing to confirm its functionality. MARCH testing might be used to look for counterfeit goods. Significant functional testing is practicable and frequently employed during production testing since memory functions are so straightforward.

- **Burn-In Test:** A burn-in test guarantees a device's reliability. High temperatures are used to run the machinery in a stressful state in order to verify reliability for an item. In order to test for infant mortality failures, unanticipated failures, and to confirm dependability, the equipment is operated at a high temperature to imitate a stressed condition. To increase confidence that the assembled unit is free of defective and counterfeit components, this can be used on the parts before manufacturing as well as to test assemblies on the production line. An extensive sequence of functional tests may reveal a fake or subpar part. Current detection processes might benefit from the addition of a functional test approach to improve the capacity to spot fake goods. A functional test requires a functioning system, often one that is PCB-based. For instance, the system could be processor-based, including memory, and have different peripherals. The functional test is a software program that uses several methods to exercise and test certain design elements. Burn-in is an essential tool since it may immediately reveal components that are marketed as military-grade but are commercial-grade. It can also get rid of components that are damaged or weren't designed to work under such pressure.
- **Structural Tests**: Over the past 10 years, a lot has changed in the way structural testing is used to lower the total value of manufacturing tests. Structural testing is especially useful for locating manufacturing errors in defective items that are out of out-of-spec or faulty. If the reverse engineering procedure reveals any discrepancies, they can identify the phony pieces. If even a tiny number of gates separates the cloned chip from the original, some of the structural test vectors will produce an incorrect result, and the CUT will be flagged as flawed. Additionally, it is feasible to detect some aging-related delays in counterfeit varieties.

3) **Aging-based Statistical Fingerprints**: Throughout their lifespan, IC performance deteriorates due to aging factors. Fake ICs will drastically reduce a device's ability to perform its critical operations for a long time when used in place of brand-new ones. There are two procedures that take use of these aging phenomena to spot repurposed fake ICs.
    - **Early Failure Rate (EFR) Data Analysis**: Since the classifier was created utilizing metrics like Vmin, Fmax, and Iddq, which are typical test results

from Early Failure Rate (EFR) evaluations required to release the majority of items, identification is carried out without incurring any additional costs. The initial step in the process of identifying fake ICs is to get a set of measurements from a reliable vendor across devices susceptible to process variations. Then, using these results of brand-new devices, a classifier is trained to distinguish between genuine and fake integrated circuits. his strategy was influenced by and is quite close to an analog/RF IC test strategy based on machine learning.

- **Circuit Path-Delay Analysis**: To distinguish between recycled and fresh ICs, a hardware-related path-delay fingerprinting approach for Trojan detection has been modified. Due to field degradation, the path-delay categorization of counterfeit ICs will differ from that of new ICs. The impacts of age on route delays may be accurately separated using statistical data analysis. The effectiveness of this approach for counterfeit IC identification is shown by simulation effects. There are three main components to the approach. First, paths are simulated, then they are selected depending on how rapidly they age. The latency of these routes is then evaluated using a clock sweeping approach in new ICs as well as in any available devices under authentication. Statistical analysis is carried out to establish if the chip under test is a counterfeit IC. The circuit undergoing authentication will go through the same test specimens that were purchased from the market in an environment that is identical. The circuit's path-delay data will subsequently be examined using the same statistical methods. The longer the circuit has been in operation, the more aging effects it will display, making it easier to detect.

VI. ΒΙΒΛΙΟΓΡΑΦΙΑ

- https://www.erai.com/CustomUploads/ca/wp/2014_6_Counterfeit_Integrated_Circuits.pdf
- https://ieeexplore.ieee.org/abstract/document/6856206
- https://personal.utdallas.edu/~gxm112130/papers/itc13a.pdf
- https://www.trentonsystems.com/blog/counterfeit-electronic-parts
- https://ieeexplore.ieee.org/abstract/document/6651880
- https://en.wikipedia.org/wiki/Integrated_circuit
- https://www.oecd.org/industry/ind/38707619.pdf
- https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file
- https://www.eng.auburn.edu/~uguin/pdfs/GOMACTech2013.pdf
- https://nepis.epa.gov/Exe/ZyNET.exe/P100BKKL.TXT?ZyActionD=ZyDocument&Client=EPA&Index=2011+Thru+2015&Docs=&Query=&Time=&EndTime=&SearchMethod=1&TocRestrict=n&Toc=&TocEntry=&QField=&QFieldYear=&QFieldMonth=&QFieldDay=&IntQFieldOp=0&ExtQFieldOp=0&XmlQuery=&File=D%3A%5Czyfiles%5CIndex%20Data%5C11thru15%5CTxt%5C00000001%5CP100BKKL.txt&User=ANONYMOUS&Password=anonymous&SortMethod=h%7C-&MaximumDocuments=1&FuzzyDegree=0&ImageQuality=r75g8/r75g8/x150y150g16/i425&Display=hpfr&DefSeekPage=x&SearchBack=ZyActionL&Back=ZyActionS&BackDesc=Results%20page&MaximumPages=1&ZyEntry=1&SeekPage=x&ZyPURL
- https://ieeexplore.ieee.org/document/5406669
- https://assets.markallengroup.com/article-images/20788/WP%20Counterfeit%20Components%20and%20Acoustic%20Microscopy.pdf
- https://link.springer.com/content/pdf/bfm:978-0-306-47040-0/1.pdf
- https://ieeexplore.ieee.org/document/1675739?denied= http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-883/s%20td883.pdf
- http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-750/s%20td750.pdf
- https://dl.acm.org/doi/10.1145/320954.320957
- https://www.sciencedirect.com/science/article/abs/pii/0045790694900175