Using Semiconductor Failure Analysis Tools for Security Analysis

Luther Martin
Voltage Security
martin@voltage.com

Abstract

Failure analysis tools like scanning electron microscopes and focused ion beam systems are commonly used in the manufacturing of modern integrated circuits. In addition to the conventional uses of these systems, they provide an adversary many ways to extract protected information from an integrated circuit and to defeat many security mechanisms that can be implemented. Since these systems are also fairly expensive, the number of adversaries with access to them is fairly limited, but it is likely that any facility capable of manufacturing modern integrated circuits also provides the capability to defeat many security features that can be implemented at the integrated circuit level.

1. Introduction

Integrated circuits are miracles of modern technology. Their manufacture requires the construction of incredibly small features that are made of ultra-pure materials, and each of the potentially millions of transistors that comprise these devices has to function properly for the device to function properly. The processes that are used to manufacture these devices are exacting, and if the processes are not performed in precisely the right way, the resulting integrated circuits may not perform to their expected specifications.

The discipline of failure analysis has evolved to correct the problems that occur in the manufacturing of integrated circuits. The first step in failure analysis is often to understand the failure mode, or the characteristics of the failure. The next step is to understand the failure mechanism, or the conditions that have created the particular failure mode. Finally, corrective action is recommended that will eliminate the failure. Failure analysis combines elements of physics, electrical engineering, material science and chemistry to accomplish this.

The investment needed to build a modern semiconductor manufacturing facility is significant and can easily reach several *billion* dollars, so integrated circuit manufacturers have great incentives to quickly diagnose and eliminate any troubles that may occur in the manufacturing process to keep their investment making products that they can sell. Because of this, very sophisticated and expensive tools have been developed to help in failure analysis. A list of commonly-used failure analysis techniques is given below in Table 1. Many of the techniques listed require expensive and specialized equipment that is rarely found outside a failure analysis laboratory, although many academic laboratories are equipped with a selection of these to support research in a specialized area. The approximate costs of representative failure analysis equipment are listed in Table 2. Because of the specialized equipment that they have, failure analysis laboratories offer a capability for analyzing integrated circuits, including discovering and exploiting any possible security vulnerabilities that they may have.

Failure Analysis Technique	Typical Application
Atomic force microscopy (AFM)	High-resolution imaging
Auger electron analysis	Surface analysis
Chromatography	Chemical analysis
Curve tracing	Current-voltage characterization
Decapsulation	Opening a packaged integrated circuit
Electron beam induced current (EBIC)	Induced current imaging of defects
Electron spectroscopy for chemical analysis (ESCA)/ x-ray photoelectron spectroscopy (XPS)	Surface analysis
Energy dispersive x-ray analysis (EDX)	Elemental analysis
Focused ion beam (FIB)	High-resolution imaging and sectioning
Fourier transform infrared (FTIR)	Chemical analysis

spectroscopy	
Hermeticity testing	Verify hermetic sealing
Laser ion mass spectroscopy (LIMS)	Compositional analysis
Light emission microscopy (LEM)	Detection of light-emitting defects
Liquid crystal hot spot detection	Detection of heat-generating defects
Microprobing	Direct electrical analysis of a circuit
Neutron activation analysis (NAA)	Detecting very small concentrations of elements
Optical beam induced current (OBIC)	Induced-current imaging of defects
Optical microscopy	Visual inspection
Residual gas analysis (RGA)	Residual gas and moisture analysis
Scanning acoustic microscopy (SAM)	Detection of delaminations
Scanning electron microscopy (SEM)	High-magnification imaging
Scanning tunneling microscopy (STM)	High-resolution imaging
Secondary ion mass spectrometry (SIMS)	Compositional analysis
Sectioning	Create a cross-section of a sample
Transmission electron microscopy (TEM)	Morphology, crystallography, and composition
Voltage contrast imaging	Detection of open conductor, lines, open or reverse-biased junctions
Wavelength dispersive x-ray analysis (WDX)	Elemental analysis
X-ray fluorescence analysis (XRF)	Elemental analysis
X-ray radiography	Internal x-ray imaging

Table 1: Summary of Failure Analysis Techniques.

Here is a brief summary of how each these failure analysis techniques works:

- AFM uses an extremely small probe that is positioned extremely close to the sample, and the deflection of the probe due to changes in topography, magnetic properties, etc., are used to construct an image of the sample. Probing with an AFM creates three-dimensional images of a sample, and does not require a vacuum for operation, but is fairly slow and is only capable of imaging a very small area.
- Auger electron analysis uses extremely low-energy electrons that are created when an electron beam interacts with a sample. These electrons come from a depth of less that 50 angstroms, so only the surface of a device can be examined with Auger analysis. An Auger system requires an extremely good vacuum for operation, and Auger systems are among the most expensive tools used for failure analysis.
- Chromatography separates a mixture into its chemical components. Chromatography is often used in failure analysis to diagnose sources of corrosion that occur in semiconductor manufacturing processes.
- Curve tracing is used to analyze the current-voltage (IV) curves of an electrical path, and is often used to characterize the breakdown voltages of p-n junctions and the gain of transistors.
- Decapsulation is used to remove the plastic or ceramic packaging of an integrated circuit to expose the die. Physical grinding can be employed to do this, as can either plasma or acid etching.
- EBIC uses the recombination of electron-hole pairs that are produced by an electron beam to image p-n junctions in a sample.
- ESCA or XPS uses x-rays to produce photoelectrons that can be used to characterize materials.
- EDX uses an electron beam to create characteristic x-rays that can be used to characterize materials.
- A FIB uses a beam of ions for either milling, cross-sectioning or deposition of material on a sample.

- FTIR uses the infrared vibrational absorption of materials to characterize them. Unlike many failure analysis techniques, FTIR does not require the sample to be in a vacuum.
- Hermeticity testing uses helium, fluorocarbon compounds or fluorescent dyes to find leaks in the package of an integrated circuit.
- LIMS uses a high-power laser to remove ions from a sample through either laser desorption or ionization that are subsequently analyzed by a mass spectrometer.
- LEM uses low-level light emissions from carrier recombination at photo-emitting defect sites to identify defect locations in a sample.
- Liquid crystal hot spot detection uses liquid crystal materials to identify defect sources that produce heat, typically from high current flow, like dielectric ruptures or metallization shorts.
- Microprobing uses fine-tipped needles that physically make contact with a sample to make voltage and current measurements that are used to diagnose failures. Waveform generators can also be attached to microprobes to provide inputs to a device under test.
- NAA uses neutron irradiation to create radioisotopes that can be detected and is capable of measuring extremely low concentrations of elements in a sample.
- OBIC uses laser photons to create current flow within a device to create an image that can be used to locate defects and anomalies.
- Optical microscopy is used to perform visual inspection of features that are difficult or impossible to perform with the naked eye, but of features that are large enough so that visible light can be used in imaging.
- RGA analysis creates a beam of ions from a gas being tested that is then analyzed by a mass spectrometer. In failure analysis, RGA is often used to identify residual gasses in a hermetically sealed package that help identify sources of corrosion.
- SAM sends an acoustic signal through a sample and uses the measured interaction with the sample to characterize it. In failure analysis, SAM is typically used to identify failures in physical connections that are made between the components of a packaged integrated circuit, like de-laminations or bond failures.
- SEM is used for high-magnification imaging that is beyond the capabilities of visible light. Although much higher resolution is possible in this way, samples in an electron microscope need to be a vacuum, so testing is much slower and the equipment is much more expensive.
- STM uses an atomically-sharp probe that is moved over a surface to create images at the atomic scale and relies on constant-current quantum mechanical tunneling to keep its probe at a fixed height. STM can also be used to move individual atoms, and is an important tool in nanosciences. STM is slow and limited to a small area, and is usually done in a vacuum to avoid contamination of the surfaces that are probed.
- SIMS uses an ion beam to produce secondary ions that are analyzed by a mass spectrometer. SIMS must be performed in a vacuum and is locally destructive.
- Sectioning uses physical cutting, grinding and polishing to expose areas of an integrated circuit for further analysis.
- TEM uses very high energy electrons that are transmitted through the sample to determine its structure.
- Voltage contrast imaging uses the interaction of an electron beam with a functioning device to obtain information about its behavior.
- WDX is similar to EDX: both use an electron beam to produce characteristic x-rays, but the detector in a WDX system counts x-rays by wavelength instead of energy, and has better resolution that EDX, although at the expense of longer time required for experiments and more expensive equipment.
- XRF uses a beam of x-rays to create characteristic x-rays, much like EDX and WDX do. Since a beam of x-rays is used instead of an electron beam, there is no damage from interaction with electrons, but the difficulties focusing x-rays limits the resolution of the technique.
- X-ray radiography is used to examine the details of a packaged device, and is often used to diagnose wirebond and die attachment problems.

Failure Analysis Equipment	Approximate Cost
Decapsulation system	$30,000
Laser cutter	$40,000
Reactive ion etcher	$60,000
Microsectioning equipment	$80,000
Microprobing station	$100,000
High-resolution x-ray system	$200,000
Light emission microscope	$200,000
Scanning acoustic microscope	$250,000
Scanning electron microscope	$400,000
Transmission electron microscope	$500,000
Focused ion beam system	$700,000
Auger microscope	$1,000,000

Table 2: Cost of Selected Failure Analysis Equipment.

To summarize the information in Tables 1 and 2, failure analysis equipment is capable of extremely detailed measurements of integrated circuits, yet at an fairly high cost. But with a full range of failure analysis tools available, it is likely that a skilled adversary can recover virtually any information from an integrated circuit, particularly when unconventional and innovative use of the available failure analysis tools is considered.

Failure analysis tools help diagnose defects in integrated circuits by determining exactly why an integrated circuit is not functioning correctly. To do this, they allow careful and detailed measurements that indicate how a device is operating, which is typically the same information that an adversary wants to obtain. Because of this, it is extremely difficult to prevent an adversary equipped with a failure analysis laboratory from recovering virtually any information that he wants from an integrated circuit. It is possible to design devices that may thwart particular techniques that an adversary may use, but typically at the expense of ease of manufacture, since the information that is denied to an adversary is also typically denied to the engineers testing the device.

The combination of expense of failure analysis tools with the significant capabilities that they provide also creates a threat model that is different than the models that have proved successful for either cryptography or software technologies. It is easy for a sophisticated adversary to develop and implement an attack against either cryptography or software security technologies and then widely distribute the tools. This has resulted in the phenomenon of “script-kiddies” who are incapable of developing attacks on their own, but are fully capable of executing software that a skilled attacker has created, and the barriers to entry are extremely low for unsophisticated attackers who want to attempt these types of attacks.

On the other hand, even the simplest attacks against hardware-based security technologies typically require the attacker to have some sort of test equipment, even if it is simple as an inexpensive logic analyzer or oscilloscope. This barrier to entry greatly reduces the number of potential attackers who might try to implement an attack against hardware-based security, restricting the potential attackers to those with the necessary engineering skills as well as the necessary test equipment.

More sophisticated attacks against hardware-based security, like the techniques that can be implemented with failure analysis tools, provide an even higher barrier to entry. These attacks require expensive and specialized equipment as well as the specialized skills needed to operate the equipment, but having the necessary equipment and skills probably provides a fairly high chance of success for defeating most hardware-based security.

The difference between the models for the protection provided by cryptography and hardware-based security are fairly different; the probability of succeeding in defeating cryptography is a monotone increasing function of the resources that we invest in an attack. The probability of succeeding in defeating hardware-based security is much different. Instead of reflecting the fact that an incremental investment in resources provides an incremental chance of success, a more reasonable model for hardware security is that a skilled adversary with access to the necessary tools has a very good chance of implementing attacks that his level of resources allows. We can somewhat arbitrarily divide attacks against hardware into four categories based on the resources available to an attacker: minimal, low, medium and high. An attacker with the resources required to perform each level of attack has a reasonable chance of success with attacks that can be carried out within their constraints.

- An attacker with minimal resources lacks either the skills or the specialized equipment to successfully carry out attacks against hardware, so their chances of success are essentially zero with almost all attacks.
- An attacker with low resources has both basic engineering skills and the test equipment needed to carry out a number of basic attacks against hardware. An experienced technician or engineer with access to a logic analyzer is an example of an adversary in this category.
- An attacker with medium resources typically has a higher level of expertise as well as access to specialized test equipment. University students and faculty as well as employees of technology companies are examples of adversaries in this category.
- An attacker with high resources has both the specialized skills and equipment to carry out the most sophisticated attacks against hardware. Experienced failure analysis engineers with access to a well-equipped failure analysis laboratory are examples of adversaries in this category. Due to the expense of the equipment required to carry out attacks that this level of technology requires, attackers in this category are probably limited to employees of large semiconductor companies and a few government-funded laboratories worldwide.

Another difference in the threat model for hardware-based security versus cryptography or software-based security is that it is usually necessary to have physical access to the hardware to implement attacks against the protection that the hardware provides, and even if an attack is successful, damage or other changes caused in the process of implementing the attack often make it extremely obvious that a particular piece of hardware has been tampered with or attacked in some way.

The time constraints of the Physical Security Testing Workshop do not permit the discussion of the potential applications of all of the failure analysis techniques listed in Table 1, so we have selected two of the techniques to further elaborate on and discuss the potential applications in the context of physical security testing: the uses of SEM and FIB systems. This remainder of this paper further describes the operation of the SEM and FIB and the ways in which these systems are used in failure analysis and ways in which these systems can be used by an adversary to defeat security features that are implemented in hardware, focusing on qualitative rather than quantitative behavior of the systems.

2. The Scanning Electron Microscope

Features of modern integrated circuits are measured in microns (um) or nanometers (nm), where 1 meter equals 10^6 um or 10^9 nm, so that 1 um equals 1,000 nm. Features smaller than 0.1 um or 100 nm are common in today's 90 nm (0.09 um) technology, technology that will be replaced by the newer 65 nm (0.065 um) technology in 2006. By comparison, a human hair is approximately 100 um in diameter, or over 1,000 times bigger than the features on a modern integrated circuit.

The energies that we encounter in failure analysis tools are often measured in electron-volts (eV), where 1 eV is the amount of energy that one electron gains when it moves through a potential difference of 1 volt. The energy of the photons in visible light ranges from 2-3 eV, and the band gap of silicon is approximately 1.1 eV. The energies of the electrons in the electron beam of a SEM or the ion beam of a FIB are much higher; energies from 0.2 keV to 30 keV are typical of a SEM while energies from 10 keV up to 50 keV are typical of a FIB.

Optical imaging systems are diffraction-limited to a resolution of approximately half of the wavelength of the light that they use. Visible light is in the range of approximately 0.4 um to 0.7 um, so conventional optical systems using visible light have a practical limit of approximately 0.2 um for features that they can resolve. Similarly, the limit to the magnification that a conventional visible-light microscope can attain is approximately 500-1,000X. Since features of modern integrated circuits are much less that 0.2 um in size, it is impractical to use visible light to view them, so more expensive systems like electron microscopes are needed.

The quantum-mechanical equivalent of the wavelength for an electron, the de Broglie wavelength, is typically approximately 0.1-1.0 nm, which is much smaller than the resolution of a SEM. In particular, the de Broglie wavelength of an electron in a SEM is given by the relationship

$$\lambda = \frac{1240 \text{ eV}\times\text{nm}}{\text{E}}$$

where E is the energy of the electron. So energy of 1 keV corresponds to a de Broglie wavelength of approximately 1.2 nm and energy of 20 keV corresponds to a de Broglie wavelength of 0.06 nm.

Other physical constraints, like the size of the electron-sample interaction, limit the resolution of a SEM, but the use of a SEM in failure analysis applications is not limited by the resolution of the system since a SEM is capable of imaging features much smaller than those present in modern integrated circuits. In addition to imaging a device, a SEM can use an electron beam to electronically stimulate the device and collect information about the way the device functions.

A SEM operates by creating a beam of electrons that is focused by a series of electromagnetic lenses into a beam that is suitable for probing a sample. The beam of electrons is generated by an electron gun. The stream of electrons from the electron gun first passes through the first condenser lens, which forms the beam, limits the beam current and reduces high-angle electrons. The beam next passes through the condenser aperture which eliminates more high-angle electrons. Next, the second condenser lens forms the beam into a tight and coherent beam that is suitable for probing a sample. An additional aperture again eliminates high-angle electrons from the beam, after which the beam passes a set of scan coils. These coils scan the beam across the sample, typically 30 times per second, dwelling on each point long enough to collect enough data to form an image. The intensity of each pixel on a display is determined by the number of interactions that are recorded by a detector as the beam dwells on a particular point. The beam then passes the objective lens which focuses the beam at the desired place on the sample. The elements of a SEM are illustrated in Figure 2.1.

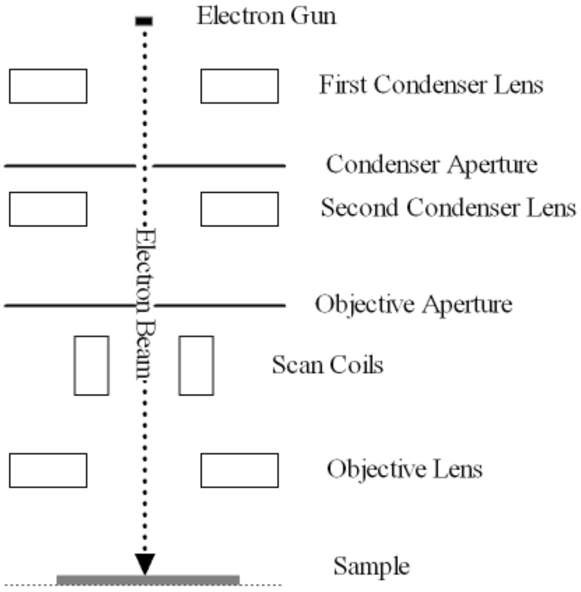

Figure 2.1: Scanning Electron Microscope Schematic.

After passing the objective lens, the electrons from the electron beam interact with the sample, interacting with both the surface of the sample as well as material within the sample. Some incident electrons produce backscattered electrons from elastic scattering from atoms in the sample. The energy of these electrons peaks at approximately 80-90% of the incident beam electrons. Secondary electrons that are the result of inelastic collisions with atoms in the sample also escape, peaking at approximately 3-5 eV. Characteristic x-rays are also produced by the interaction of the electron beam with the sample, so it is also possible to determine the chemical composition of the sample by analyzing the characteristic x-rays that interaction with the electron beam produces. The interaction of the electron beam with a sample is illustrated in Figure 2.2.

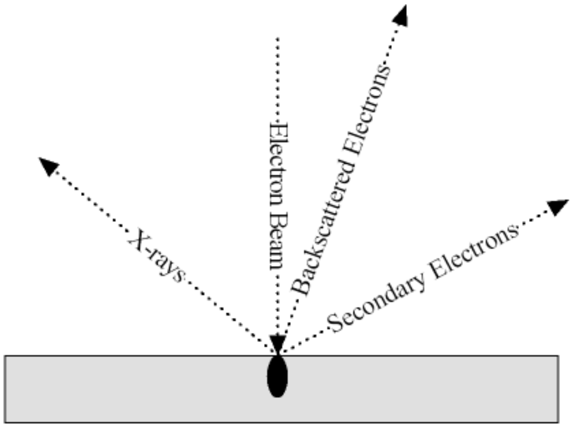

Figure 2.2: Interaction of Electron Beam with a Sample.

A typical SEM is operated with an accelerating voltage of between 0.2 kV and 30 kV, which produces a spot size of between 1 nm and 7 nm on the sample. A small spot does not necessarily guarantee better resolution, however, since the interaction volume from which secondary electrons are collected also affects the resolution. A higher beam energy (E) gives a bigger interaction volume, which tends to lower the resolution that is possible, while a higher atomic number (Z) for the material comprising the sample gives a smaller interaction volume. This is illustrated in Figure 2.3. The typical resolution of a SEM is approximately 3 nm, and magnifications of up to 300,000X are possible.

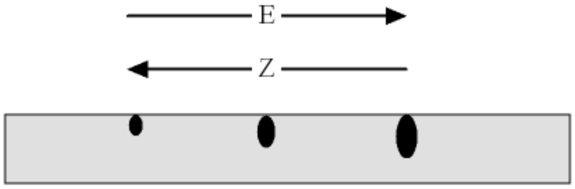

Figure 2.3: Electron Beam Interaction Volume.

Although a SEM can resolve much smaller features than a visible-light microscope can, a SEM needs to be operated at a very low pressure, typically a vacuum of approximately 10^{-6} torr. The low pressure is needed to keep the filament of the electron gun from burning out, and it is also needed to allow the electrons comprising the electron beam to reach the sample unimpeded, and prevents unwanted gas molecules from accumulating on the sample surface. The beam current in a typical SEM is 10-15 pA, or approximately 10^8 electrons per second.

To create an image from secondary electrons, a detector near the sample counts the number of secondary electrons that are collected while the electron beam dwells on a particular spot on the sample, as shown in Figure 2.4. The intensity of a pixel of the image is proportional to the number of electrons that are collected by the detector while the beam dwells on the corresponding part of the sample.

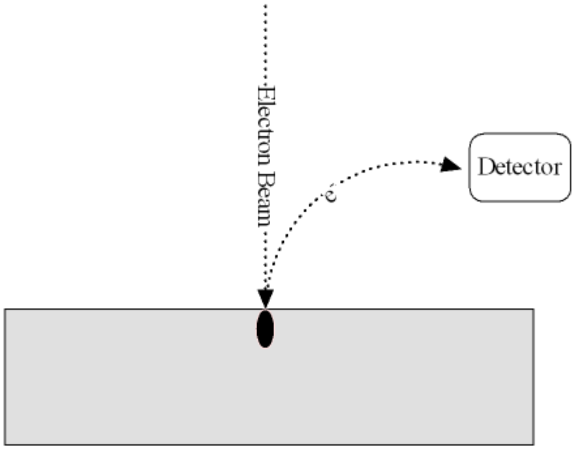

Figure 2.4: Secondary Electron Detector.

When the electron beam of a SEM interacts with an integrated circuit when the integrated circuit is operating, we find that the interaction between the functioning device and the electron beam becomes the major source of contrast in the resulting image. When device features below the interaction of the electron beam are at a high electric potential, secondary electrons are more tightly held to the surface of the device, and when the potential is lower, these additional secondary electrons are more easily knocked off the surface and collected by the detector. This is illustrated in Figures 2.5 and 2.6. By recording the variations in the collected secondary electrons over time, it is possible to measure the signals that are propagating through an integrated circuit, and equipment that is optimized for collecting this type of data is widely used in the testing and failure analysis of integrated circuits.

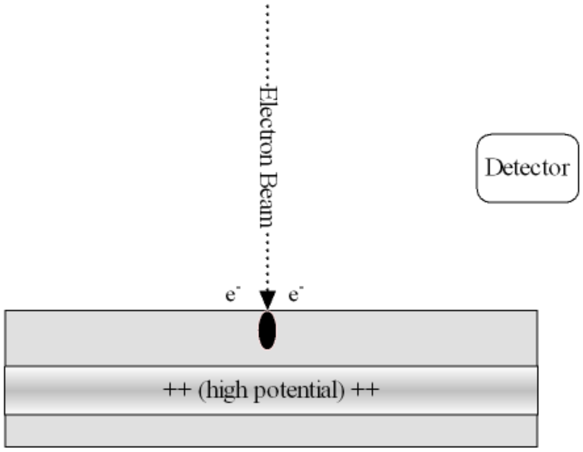

Figure 2.5: Voltage Contrast Imaging over High Potential.

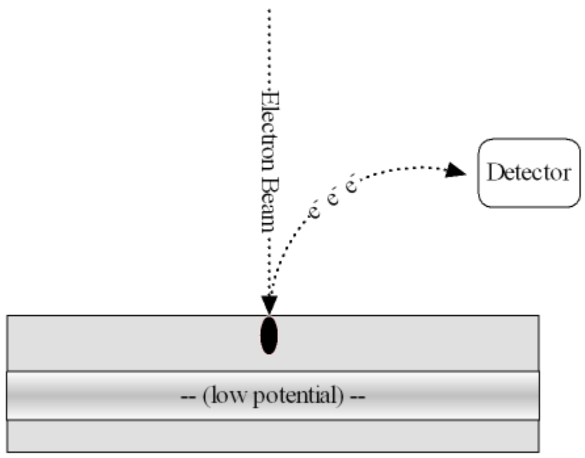

Figure 2.6: Voltage Contrast Imaging over Low Potential.

The main application of a SEM to security analysis of integrated circuits is either using voltage contrast imaging to observe the operation of parts of a device or to collect waveforms from a functioning device. So although it is not always possible to attach mechanical probes to an integrated circuit, it is often possible to collect the same type of data that physical probes would provide from an operating device. This makes it possible for an adversary to learn a great deal about the operation of the device. In particular, by collecting data on the internal data bus of an integrated circuit it is possible to determine what data is being transmitted, either between functional elements of a device or as data is read to memory or read from memory.

Cryptographic keys, for example, are often stored in a secure location but loaded into some sort of register for use, and it is possible to read the value of the bits comprising a key as it is moved from one location to another on the internal data paths of an integrated circuit. So it may be possible for an adversary to extract data that is otherwise protected just by probing with an electron beam as a device operates, even if the storage and use of the cryptographic key follows best practices.

3. The Focused Ion Beam System

A FIB system operates very similarly to a SEM, except for one major difference: a beam of positive gallium ions is created instead of a beam of electrons. A gallium ion is approximately 50,000 times heavier than an electron, and the increased mass of the gallium ions lets them to dislodge or sputter material from the sample in the form of either ions or neutral atoms where the ion beam interacts with the sample. Secondary electrons are also produced by the interaction of the incident ions with the sample. Many more secondary electrons are created than dislodged atoms, and the collection of secondary electrons in a FIB system can be used to create images similar to the ones created in a SEM. The interaction of the ion beam with the sample is summarized in Figure 3.1. The spot size of a FIB is typically approximately 4 nm, and the typical resolution is approximately 7 nm.

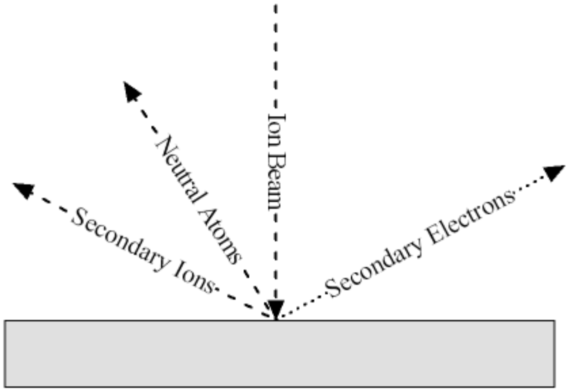

Figure 3.1: Interaction of Ion Beam with a Sample.

The interesting uses of a FIB system involve the interaction of the ions with the sample. By repeatedly scanning the ion beam over a fixed area, the material comprising the sample can be sputtered away as shown in Figure 3.2. This provides an easy way to remove layers of a device to examine or probe the lower structures. Re-deposition of the sputtered material can be a problem, and experiments with integrated circuits need to be carefully designed to avoid the complications that this can cause.

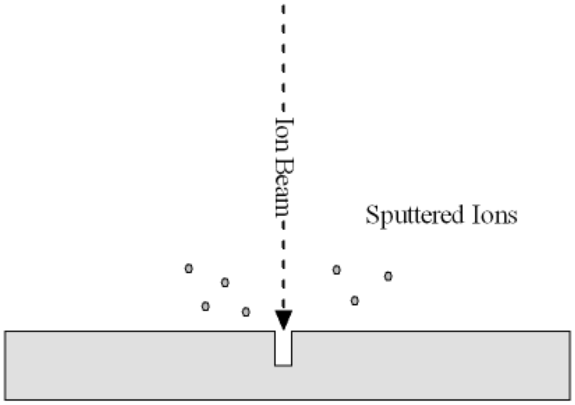

Figure 3.2: Ion Milling.

By introducing different types of gasses into a FIB system, it is possible to either enhance the removal of material from the sample or to selectively deposit material on the sample. If small amounts of a halogen or a halogen-containing gas are directed at the sample and the beam energy is adjusted correctly, it is possible to cause a reaction between the sputtered material and the gas molecules that forms a volatile product that minimizes redeposition. This technique is called gas-assisted etching, and it allows increased milling rates and better aspect ratios of milled areas than are possible otherwise. In addition, by changing the composition of the gas introduced it is possible to preferentially etch particular materials that are used in an integrated circuit. So it is possible to use gas-assisted etching to selectively remove thin dielectric layers without damaging the underlying circuitry, or to selectively remove metal lines without damaging the underlying interlevel dielectric.

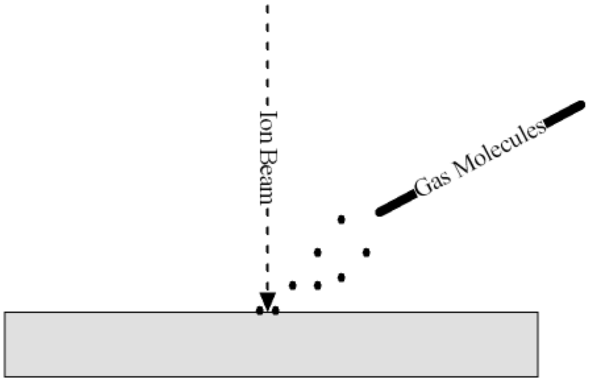

Figure 3.3: Ion-induced Deposition.

It is also possible to use an ion beam to selectively deposit materials on a sample, like shown in Figure 3.3. To deposit materials, the beam energy is adjusted so that the sample acquires energy below the sputtering threshold. To deposit metal, an organo-metallic gas, typically $W(CO)_6$, is introduced, and the interaction of the ion beam with the gas produces an non-volatile product that deposits on the sample. Repeated scanning of the ion beam over an area of the sample results in the deposition of a layer of tungsten that can be used to make electrical connections of one part of the sample to another.

If a siloxane gas, typically methyl siloxane, or CH_2SiO, is introduced along with oxygen, it is possible to selectively deposit an insulating layer of silicon dioxide, SiO_2, on a sample. The capability to deposit insulating layers, along with the capability to deposit conductors and to remove material from a sample, makes complex modifications, or microsurgery, to integrated circuits possible as shown in Figure 3.4.

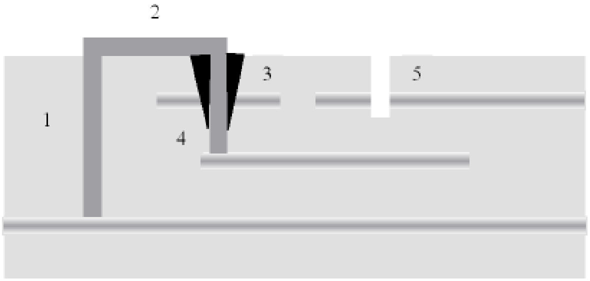

Figure 3.4: FIB Microsurgery on an Integrated Circuit.

Figure 3.4 illustrates applications of a FIB system to perform microsurgery on an integrated circuit. Modification (1) shows where an ion beam with gas-assisted etching has been used to mill a high aspect ratio hole to a buried metal layer that which has then been filled with tungsten. Modification (2) shows where a deposited layer of metal has connected the two connections to the buried metal layers. Modification (3) shows where deposition of a dielectric allows the creation of a tungsten connection (4) to a lower metal layer through an upper metal layer. Modification (5) shows a hole that cuts a buried metal line.

FIB microsurgery is an extremely valuable tool for an adversary who is attempting to defeat security mechanisms that an integrated circuit provides. By cutting metal lines it is possible to physically disconnect circuitry that implements security functions. By milling holes to metal lines, even ones that are buried below many other layers, and then laying a conducting connection to either power or ground, it is possible to either permanently enable or disable circuitry. This can give an adversary the ability to selectively disable many security features that are implemented in hardware.

Another application is probe pad creation, in which we mill a hole to a buried metal line and then connect the metal line to a metal pad that is deposited on the uppermost layer of dielectric, thus providing a way to monitor the data being transmitted over the hidden line by voltage contrast imaging or microprobing.

4. Summary

The capital-intensive business of manufacturing integrated circuits is enabled in part by an extensive array of failure analysis tools that are capable of recovering virtually any information from an integrated circuit. It is difficult to implement strong security in hardware for two reasons. Denying information to adversaries also may deny the same information to test engineers, and thus make the manufacturing of the technology more difficult and expensive, and techniques that are designed to thwart a particular attack may often be vulnerable to attacks by other means. Because of this, the threat model for hardware-based security is probably fundamentally different from the threat models that have been developed for other technologies.

5. References

Giannuzzi, Lucille A.; Stevie, Fred A. (Eds.). *Introduction to Focused Ion Beams: Instrumentation, Theory, Techniques and Practice*. New York: Springer, 2005.

Goldstein, J., Newbury, D.E., Joy, D.C., Lyman, C.E., Echlin, P., Lifshin, E., Sawyer, L.C., Michael, J.R. *Scanning Electron Microscopy and X-ray Microanalysis*, New York: Springer, 2005.