Digital Forensic Atomic Force Microscopy of Semiconductor Memory Arrays

Struan Gray, Stefan Axelsson

Chapter 12

DIGITAL FORENSIC ATOMIC FORCE MICROSCOPY OF SEMICONDUCTOR MEMORY ARRAYS

Struan Gray and Stefan Axelsson

Abstract Atomic force microscopy is an analytical technique that provides very high spatial resolution with independent measurements of surface topography and electrical properties. This chapter assesses the potential for atomic force microscopy to read data stored as local charges in the cells of memory chips, with an emphasis on simple sample preparation ("delidding") and imaging of the topsides of chip structures, thereby avoiding complex and destructive techniques such as backside etching and polishing. Atomic force microscopy measurements of a vintage EPROM chip demonstrate that imaging is possible even when sample cleanliness, stability and topographical roughness are decidedly suboptimal. As feature sizes slip below the resolution limits of optical microscopy, atomic force microscopy offers a promising route for functional characterization of semiconductor memory structures in RAM chips, microprocessors and cryptographic hardware.

Keywords: Atomic force microscopy, memory chip delidding, surface imaging

1. Introduction

Atomic force microscopy has been used to investigate the structures of memory devices and to conduct detailed failure analyses of memory cell structures. However, limited information is available about the use of atomic force microscopy to read the memory content of packaged chips. The published information suggests that atomic force microscopy and related techniques should work – the open question is how well.

The initial results presented in this chapter reveal that, even without custom sample mounting or modification of the atomic force microscope itself, it is possible to obtain topographic data from a packaged chip

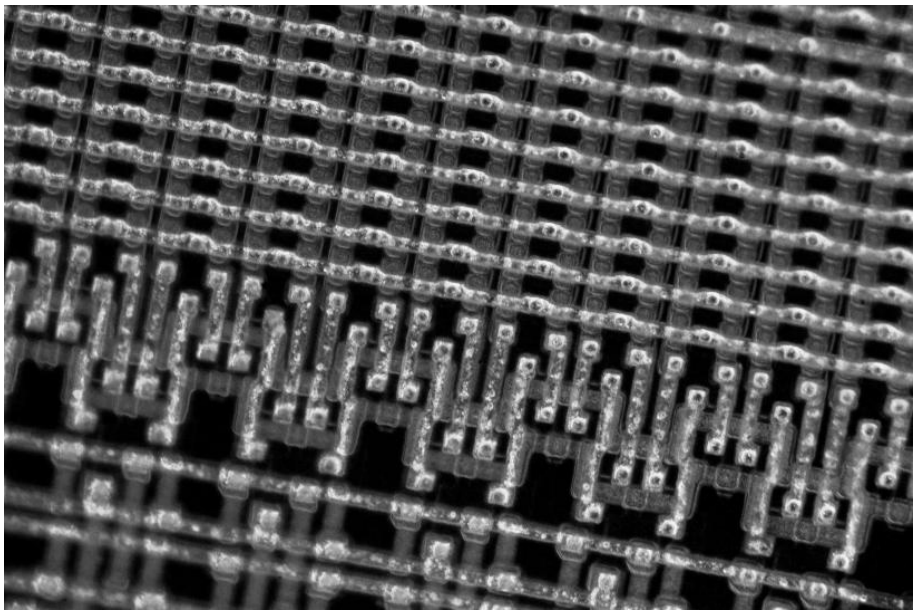

Figure 1. EPROM memory circuits imaged by dark-field optical microscopy.

using a basic research-grade instrument (Figure 1). Should future work prove the feasibility of the technique, it is easy to envision the creation of a custom atomic force microscope that could accommodate integrated circuits *in situ* on circuit boards. A key aspect of investigations in this area would be to perform topside imaging and characterization, avoiding the need for backside polishing and etching and, in principle, maintaining the integrity of the chip as a working device.

There are some interesting prospects for the future. Micro-electromechanical systems (MEMS) technology and other manufacturing processes, which could produce smaller, lighter atomic force microscopy structures with higher fundamental resonance, would enable an increase in data access rates and crash-free investigations of surfaces with high relief. These, in turn, would impact the practicability and security of the applications discussed in this chapter. Further development of high-speed electronics and microwave engineering may permit other advances in surface characterization of semiconductor devices or simply make measurements easier, cheaper and more reliable.

From the point of view of forensic investigations, atomic force microscopy offers a number of advantages: it is minimally invasive; it may be performed in a wide variety of environments; and it can be used to image almost any kind of sample. The problems in performing atomic

force microscopy studies of working memory chips are mostly practical, but are of sufficient severity to deter casual investigations. Whatever the future may bring in terms of instruments and their capabilities, one thing is clear: sample preparation techniques will continue to be very important.

This chapter focuses on atomic force microscopy and related techniques, and how future developments could make them more applicable to forensic investigations of memory chips. The results of preliminary experiments are used to illuminate the practical issues that limit successful implementation.

2. Background

This section discusses probe microscopy and relevant issues related to security and forensics.

2.1 Probe Microscopy

Probe microscopy has antecedents in various stylus-based surface profiling tools, but the dramatic increases in sensitivity and resolution provided by the invention of scanning tunneling microscopy (STM) in 1981 [4] have led to the explosive development of instruments and their applications. Atomic force microscopy (AFM) was invented soon afterwards [3], motivated by a desire to expand the atomic resolution of the scanning tunneling microscope to investigations of non-conducting samples. Atomic force microscopy uses a force interaction between the probe tip and the sample surface to measure the distance between them. Typically, the interaction involves the Van der Waals force, but in principle, any force that varies with the relative positions of the tip and sample may be employed.

The narrow focus on atomic resolution as the ultimate goal of probe microscopy has ensured that the early literature in the field is full of interesting experiments and phenomena that failed to make an impact because of what was perceived as "poor resolution." Many of these techniques have been justifiably neglected, but some loiter at the margins of respectability and are worth revisiting periodically to examine whether or not they have acquired contemporary relevance. An example is using microwave or radio-frequency signals to measure the electrical characteristics of a sample surface. This was proved to be possible in the early days, but the methods were not robust enough to be adopted widely. However, novel measurements made recently using scanning microwave impedance microscopy (SMIM) have rejuvenated the field, revealing spatial variations in surface capacitance with nanometer resolution [15].

In addition to scanning microwave impedance microscopy, two more established techniques – electrical force microscopy (EFM) and scanning capacitance microscopy (SCM) – are relevant to forensic investigations of chip surfaces. All three techniques use the voltage on a conductive tip to reveal additional information about a surface beyond its topography. Electrical force microscopy measures the Coulomb forces between the tip and any charge concentrations on the sample surface. Scanning capacitance microscopy uses a modulated voltage to reveal changes in the tip-surface capacitance that are related to local doping levels, stored charge and metallization of semiconductor devices. Scanning microwave impedance microscopy investigates similar factors by regarding the tip-sample junction as the termination of a transmission line using the back-reflected signal to measure the complex tip-sample impedance.

2.2 Security and Forensics

Secure communications and computing have been important for many years and their importance seems set to increase. Several techniques have been devised to defend against attacks on confidentiality, integrity and availability. These include the use of cryptography [22], information flow analysis [23], and detection and estimation theory [1]. The vast majority of these techniques depend on a secure "black box" to hide the secrets or to perform computations. The concept takes different names depending on how it is implemented, including trusted computing bases in secure operating systems [20], bastion hosts in firewalls [19] and trusted platform modules in hardware-supported security [12].

In the case of secure operating systems and firewalls, many types of attacks are known, for example, those based on the exploitation of (inevitable) software flaws. Likewise, a number of attacks against hardware have been devised, many of them based on observing, or affecting, the hardware operating environment. The attacks include differential power analysis [13], differential fault analysis [2], probing with light/laser excitation [21], freezing of memory [10], electron microscope analysis [17] and Van Eck/TEMPEST radiation analysis. All these attacks, with one or two exceptions, require physical access to the hardware. Physical access is becoming increasingly easy to obtain as secure electronic hardware in the form of embedded and mobile devices is becoming commonplace. As these devices, especially those in mobile phones, have become ubiquitous, increased security requirements have led manufacturers to rely on hardware-based cryptographic modules and ubiquitous encryption to maintain the security of user data [9]. This has presented significant challenges to law enforcement and other actors who need to access the

stored data in order to investigate crimes and other incidents. While there has been some success in leveraging software flaws in security implementations of smartphones, it is unclear how long this avenue will remain effective [8].

It follows that other techniques, including piercing the black box itself using sophisticated analysis techniques, are probably the inevitable next step in the evolution of digital forensics. However, it should be noted that knowledge pertaining to such attacks is not only useful to would-be attackers (e.g., law enforcement), but also to defenders, because it is difficult to defend against unknown threats. One such threat that should not be ignored is the question of whether or not the hardware can be trusted, especially if backdoors have been introduced during the manufacturing process [24].

3. Atomic Force Microscopy

Before examining more specialized techniques and how they have been applied to investigations of semiconductor memory devices, it is instructive to summarize the benefits and problems of atomic force microscopy because they are relevant to all derived technologies. Atomic force microscopy is a mature technique and the purpose here is not to reproduce the wealth of information in the numerous textbooks, manufacturer application notes and (surprisingly reliable) Wikipedia entries. Instead, the technique is briefly described with an emphasis on key performance metrics that are relevant to digital forensics as well as aspects that are currently limiting, but where future developments could have significant impact.

Figure 2 shows a generic atomic force microscopy setup in which a laser is reflected from the back of a cantilever carrying a sharp tip. A split photodiode measures the deflection of the laser beam, which changes as the cantilever flexes in response to the forces between the tip and the sample. The deflection signal is fed to a feedback loop that adjusts the position of the cantilever mount to keep the force and, hence, the height above the surface constant. As the tip moves sideways, its position tracks changes in the surface topography while the feedback loop maintains a constant height.

Most routine work has stabilized around the use of probes manufactured via semiconductor microfabrication techniques, with the tip and cantilever integrated in a standardized chip. The stiffness and other mechanical properties of the cantilever can be readily tuned; other aspects of the tip can also be optimized for particular applications. For example, conductive tips for the techniques discussed in this chapter can be

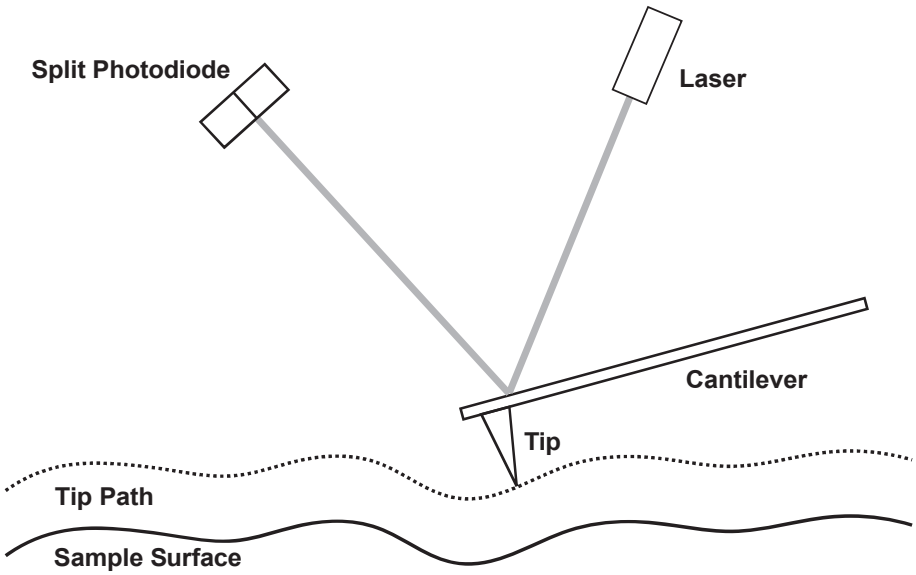

Figure 2. Atomic force microscopy.

made by doping the semiconductor material used in their manufacture or by evaporating metals onto the structure. Cantilevers typically have force constants ranging from 0.1 to 100 N/m depending on their intended modes of operation. Typical atomic force microscopy resolutions are 0.1 to 10 nm vertically (largely limited by noise) and 1 to 100 nm laterally (largely limited by tip shape, and tip and sample quality).

Sensing position via the static flexing of the cantilever – the so-called "contact" mode – is an option for most microscopes, but the forces between the tip and sample tend to be large, often leading to damage or wear. It is more common to situate the tip farther away from the surface, where the forces are weaker, using a modulation technique to recover sensitivity. Such oscillation-based schemes are robust and reliable; because the tip spends most of its time far from the surface, the potential for wear or damage are reduced substantially. A high-amplitude oscillation also ensures that strong interactions at close distances (e.g., adhesion or attraction to an absorbed water layer in ambient conditions) do not cause substantial dragging or friction, enabling rough and unpredictable surfaces to be measured more easily.

Oscillatory schemes also enable forces other than the intrinsic Van der Waals interaction to be distinguished, for example, by modulating them with a different frequency, or because they operate out of phase or have a different gradient with respect to the distance from the sample. Thus, when measuring Coulomb forces in electrical force microscopy,

it is possible to modulate the voltage on the tip at a frequency well below that of the cantilever oscillation and, thus, use a second lock-in measurement to assess the electrostatic force separately.

The most widely-quoted figures of merit for atomic force microscopy and related techniques usually involve resolution. This, as mentioned above, can be something of a distraction. Even a desktop atomic force microscope operating in air at standard temperature and humidity can readily achieve 10 nm resolution, provided that the sample surface is clean and stable. Although gate lengths and some oxide thicknesses in semiconductor devices are approaching these dimensions, the lateral spacing of any likely two-dimensional storage structure is considerably larger and it is not likely that the spatial resolution limit of atomic force microscopy would present a significant obstacle to determining whether or not a given memory cell is charged.

Other aspects of atomic force microscopy are likely to be more significant than resolution, especially bandwidth and the time domain. There are three key timescales that govern how an atomic force microscope measurement may be made. Perhaps the least significant is the most fundamental: all electromagnetic and chemical interactions between the tip and surface operate on a timescale determined by the propagation of electromagnetic energy in the near field and the response times of electrons and other charges in the materials. Typically, this corresponds to frequencies in or beyond the visible spectrum (10^{14} Hz or higher), which implies a typical timescale of femtoseconds or less. Two firm conclusions can be made because the timescale is so much faster than any near-term developments in clock speed or phase-coherent detectors. First, any experiment that is devised is unlikely to be limited by the fundamental electromagnetic properties of the materials, even at terahertz frequencies. Second, if the response to higher frequency stimulation is of interest, then a modulation scheme or some sort of heterodyne detection would be needed to shift the signal into a measurable band.

The most significant timescale for practical experiments, including digital forensic uses, is the pixel clock: the rate at which an atomic force microscopy system can take individual pixels of the final image. This is surprisingly slow: typical times for a raster scan are 0.1 to 1 seconds for each line of data, leading to acquisition times of an hour or more even for low-resolution images. The slow response is set by the fundamental mechanical frequency of the microscope as a whole. This limits the response to positioning commands from the feedback loop and scan drivers because operating above resonance with an unknown mechanical phase shift quickly leads to unrecoverable damage to the sample and/or tip. The rigidity of the microscope is determined by

factors related to its intended use and special instruments can achieve better performance by dispensing with easy tip exchange or the need to accommodate a wide range of sample sizes.

This factor is also the one that may be most amenable to change and where developments directly applicable to forensic imaging are expected. For example, efforts are underway to use micro-electro-mechanical systems technology to make the entire atomic force microscope exchangeable rather than just the tip [16]. Integrating the motion actuators, cantilever and tip in a monolithic package can make the mechanical loop between substrate and tip considerably smaller and stiffer, raising its fundamental frequency and enabling faster scanning while still under closed loop control.

Faster scan speeds will allow more rapid processes to be recorded and studied, as well as make scanning more reliable and tip crashes less likely. As discussed in the pilot study below, the slow response of current microscopes is not only frustrating, but it leads to poor quality data. Improving predictability and reducing the likelihood of damaging the sample under study will only benefit digital forensic investigations in search of presentable evidence.

The third important timescale is the fundamental oscillation frequency of the cantilever. This is adjustable based on design and materials, but the usual value lies in the 100 to 300 kHz range. At present, this is not regarded as a limitation. Other signals can be modulated at 1 to 50 kHz and still be safely below the oscillation frequency while remaining well above the pixel clock rate. There may, however, be difficulties in the future. If, as is highly desirable, scan speeds increase and raise the pixel clock rate, limited bandwidth will be available for intermediate frequency measurements in electrical force microscopy, scanning capacitance microscopy and scanning microwave impedance microscopy.

One final property of atomic force microscopy is of relevance. Unlike an electron microscope with its relatively high beam energy or even a visible light microscope that uses photon energies capable of breaking chemical bonds, an atomic force microscope has a very soft touch. It is possible to use forces so low that any sample sensitive to them would be impractical as a device. It is also possible to measure electrical characteristics with extremely low applied voltages, currents and fields. This makes atomic force microscopy excellent for non-destructive testing and also makes it difficult to implement countermeasures in the chips being investigated.

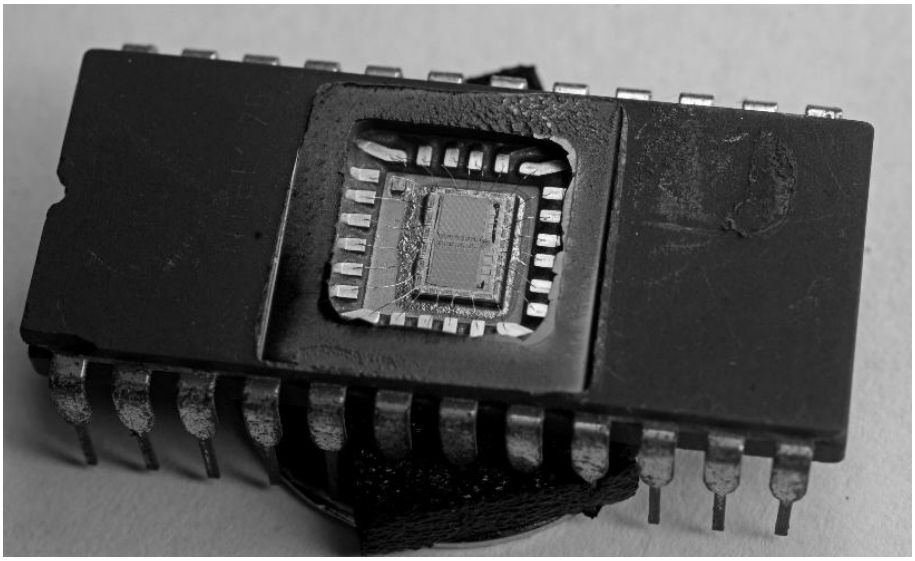

Figure 3. EPROM memory chip with exposed die (approx. 4 mm×8 mm in size).

4. Memory Chip Layout and Structure

Like most semiconductor integrated circuits, memory chips are created by cycles of lithography, deposition and reaction to produce fine-scale patterns of various materials on the surface of a single-crystal semiconductor wafer, usually silicon. The basic chip or die is brittle and sensitive to chemical and mechanical damage, so it is usually packaged before being used in a device. First, thin wires are bonded to the chip die to create more robust connections to metal pins than can be accomplished using conventional soldering techniques. Next, the die and cage are encapsulated. Polymer resins are now used for packaging; sintered ceramics used to be common and are still employed in some devices.

Figure 3 shows a 1,024 B Intel 2708 EPROM memory chip made in 1974. The exposed chip die is approximately 4 mm×8 mm in size. Despite its venerable age and low capacity, the chip illustrates the general characteristics that are still shared by modern high density devices. The quartz window that protects the chip die has been removed to show the structure beneath it. Because the circuits etched into the chip surface are so large, they are easy to see with a camera lens or microscope.

Figure 4 shows a close-up view of the die itself. The two large blocks are the actual memory locations, which are surrounded by control circuitry and address lines used to write and read data. The figure also shows the bonding pads to which thin bonding wires are attached.

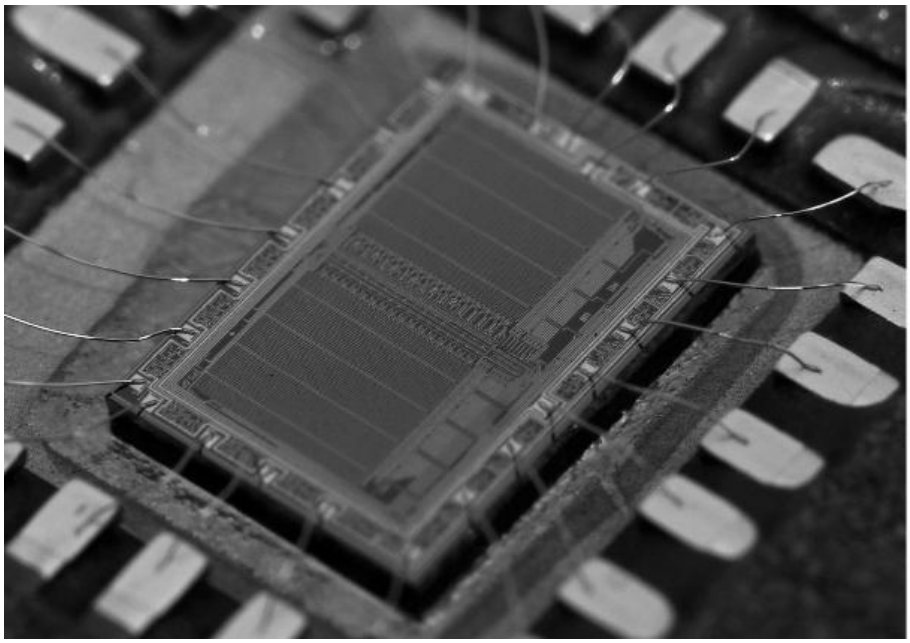

Figure 4. Close-up view of the chip die showing two arrays of memory cells.

The first lesson, which is also relevant to modern, high-density surface-mount integrated circuits, is that the overall package is much larger than the die itself. The second is that a substantial 3D structure surrounds the planar circuits on the die; this means that access to the memory array has to take place through a tunnel cut in the packaging and between the arcs of the bonding wires. This is by no means trivial for probe microscopy because non-standard or extended mounting of the cantilever impacts imaging performance.

Figure 5 shows an optical microscope image of the individual memory arrays. Charge is stored in the oval structures and electrical connections are made to a single memory cell by addressing the appropriate combination of white and yellow/gold lead-in traces. The spacing between the bright white address lines is approximately $20\,\mu$m. Modern chips are more complex and have structures that are an order of magnitude smaller. Also, they often include more transistors and other active devices as part of the individual memory cells. However, the general layout of memory chips is very similar as is the packaging.

5. Prior Art

The three atomic force microscopy techniques – electrical force microscopy, scanning capacitance microscopy and scanning microwave im-

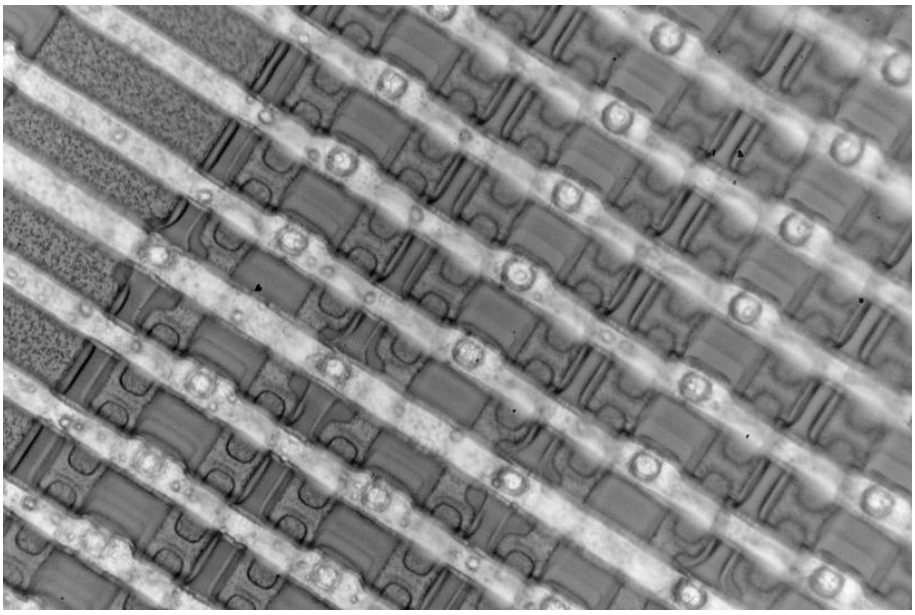

Figure 5. Optical microscope image of individual memory cells.

pedance microscopy – all have potential for investigations of semiconductor memory. They use a conductive tip to apply or sense electrical signals and typically employ conventional atomic force microscopy height sensing to control the tip position while measuring the electrical signals independently.

The first technique, electrical force microscopy, measures the electrical forces between a surface and a charged tip. An oscillating voltage is often applied to the tip and a lock-in amplifier is used to isolate this component of the signal coming from the split photodetector. Provided a frequency is chosen that lies between the pixel clock and the fundamental frequency of the cantilever, this perturbation neither affects the topographic image data nor the basic operation of the height stabilizing feedback. The lock-in signal represents the gradient of the electric force on the tip with distance. This signal changes sign when the tip is over positively or negatively charged regions of the surface. Although absolute quantitative measurements require detailed 3D models of the tip, surface geometry and materials, it is possible to map electric field gradients due to local charges.

The application to semiconductor memory devices is obvious because charges are mostly stored in capacitors or floating gate electrodes, which produce fringing fields that affect nearby sensing electrodes. Typical

charge and discharge voltages are much larger than the tip voltages needed for good signal-to-noise in electrical force microscopy, so a measurement can be made without erasing the charge structure on the sample surface. Measuring the difference between a memory cell with a charged floating gate and a cell with a neutral gate is well within the capabilities of most instruments.

There is little reported work on using electrical force microscopy to image and read the contents of packaged semiconductor memory. An application note by Park Systems [18], a commercial manufacturer of atomic force microscopes, reports electrical force microscopy measurements on bare, unpackaged, uncontacted memory cells. Reports are also available about materials-science-oriented studies focused on developing novel memory structures (see, e.g., [6, 11]). However, these works do not describe successful top-down measurements of mainstream memory devices. Konopinski [14] has conducted the most extensive electrical force microscopy investigation of memory arrays, specifically flash memory EEPROMs used in SIM cards. While the electrical force microscopy measurements in this study were inconclusive, they do not rule out the utility of the technique.

The second technique, scanning capacitance microscopy, imposes a DC bias on the conducting tip with an overlaid oscillatory voltage. The currents on and off the tip are measured using a preamplifier placed close to the cantilever; a lock-in technique is used to provide specificity and noise rejection. The signal yielding the scanning capacitance microscopy measurement is proportional to dC/dV at the DC bias voltage. The technique is most applicable to systems where dC/dV varies with voltage, which includes many semiconductor structures.

Scanning capacitance microscopy has been used extensively to characterize on-chip transistor and memory structures in cross-sectional and top-down planar views. In fact, most manufacturers of commercial microscopes that offer scanning capacitance microscopy as an option provide an SRAM chip as a test sample. However, as in the case of the Park Systems technical note [18], the emphasis is usually on imaging a passivated planar sample with no actual connections to the doped regions of the semiconductor instead of *in situ* measurements of connected charged devices. The most attractive use of scanning capacitance microscopy is to assess dopant levels in semiconductors. It can reliably and robustly detect the difference between n-type and p-type regions. With suitable modeling, it is also able to measure doping levels as a function of position across the surface.

Some studies have used scanning capacitance microscopy to read the contents of memory cells. De Nardi et al. [7] have successfully used

scanning capacitance microscopy to read memory devices that were extensively prepared for the scanning capacitance microscopy technique. They were able to distinguish between cells containing bit values of 1 and 0, and to recreate word-length data from scanning capacitance microscopy images. They also emphasize the need to map the physical locations of the data as seen by scanning capacitance microscopy to their logical locations within the conceptual data array. This is one area are where countermeasures such as scrambling physical memory locations on an individual chip could defeat read attempts. However, in cases where a consistent layout is used, the mapping can be performed for a single device (other than the device under test) and the results could be applied to all the devices in the same batch or of the same type.

The scanning capacitance microscopy study by De Nardi et al. [7] and the electrical force microscopy study by Konopinski [14] both involved the extraction of the die from the memory device and thinning it from the backside, reducing the chip thickness until the underside of the active circuits was almost exposed. This is not a trivial procedure, but is necessary, especially in the case of scanning capacitance microscopy, which relies on band-bending induced by the electric field from the tip to create a signal. In any case, it is essentially impractical to take measurements from the topside through the arrays of addressing and control lines.

The third technique, scanning microwave impedance microscopy [15], uses matched transmission lines and filters to apply a microwave signal to the conducting tip. A conventional RF network analyzer then records the back-reflected signal, essentially treating the tip-sample junction as an unmatched termination to the transmission line. From this, it is possible to extract the complex impedance of the junction and map it across the surface. As with scanning capacitance microscopy, the oscillatory signal enables the impedance measurement to be decoupled from the topography; the output signal is proportional to dC/dV for the imaginary part and to dR/dV for the real part. Scanning microwave impedance microscopy provides similar information as scanning capacitance microscopy, but with greater reliability and signal-to-noise. The published literature on scanning microwave impedance microscopy is a little thin, but the technique has definite promise.

6. Vintage EPROM Chip Experiments

The experiments involved preparing and mounting a 1,024 B Intel 2708 EPROM memory chip in an atomic force microscope in order to investigate whether or not topside measurements are possible without the

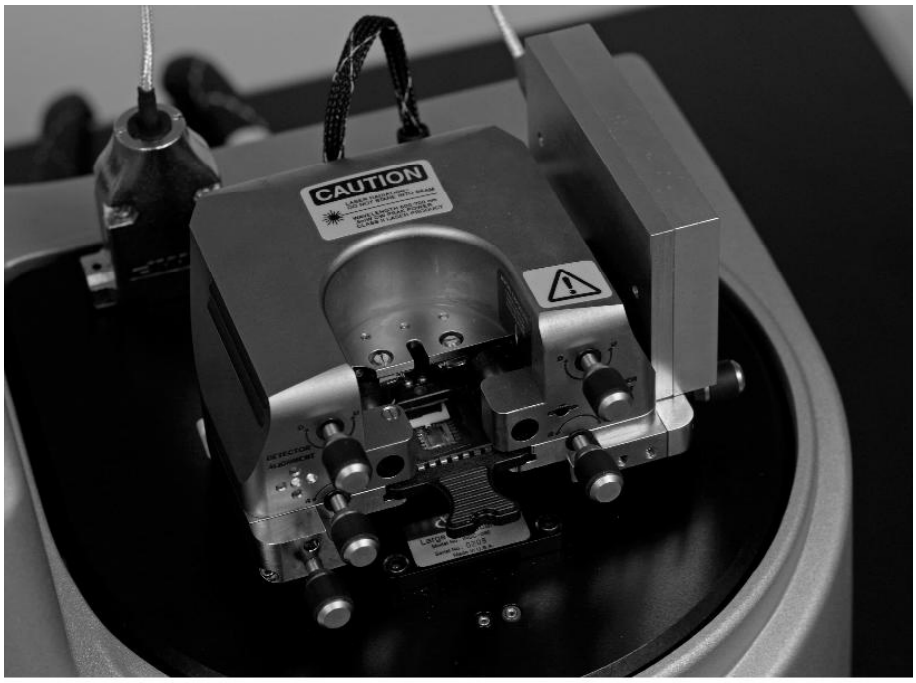

Figure 6. Innova microscope with the EPROM chip mounted.

extensive and destructive sample preparation described in the electrical force microscopy and scanning capacitance microscopy studies discussed above.

The experiments employed an Innova atomic force microscope, a low-cost research-grade instrument, with scanning capacitance microscopy capabilities [5]. The atomic force microscopy system has a built-in video microscope that enables the tip position to be correlated with measurements using other microscopes. The system can perform atomic force microscopy on areas up to $100\,\mu\text{m} \times 100\,\mu\text{m}$ in size.

Figure 6 shows the Innova atomic force microscope with its soundproof cover removed and the EPROM chip mounted on the sample stage. The electronics for the scanning capacitance microscopy preamplifier are housed in the gold-colored rectangular box on the right.

Figure 7 shows a close-up view of the chip mounted *in situ* in the Innova atomic force microscope. The cantilever chip is mounted in the white holder at the top center. The red laser used for deflection detection can be seen reflecting off the cantilever itself, with some stray light to the left and on the surface of the EPROM chip. It is clear that space is extremely tight. Also, the rear of the atomic force microscope

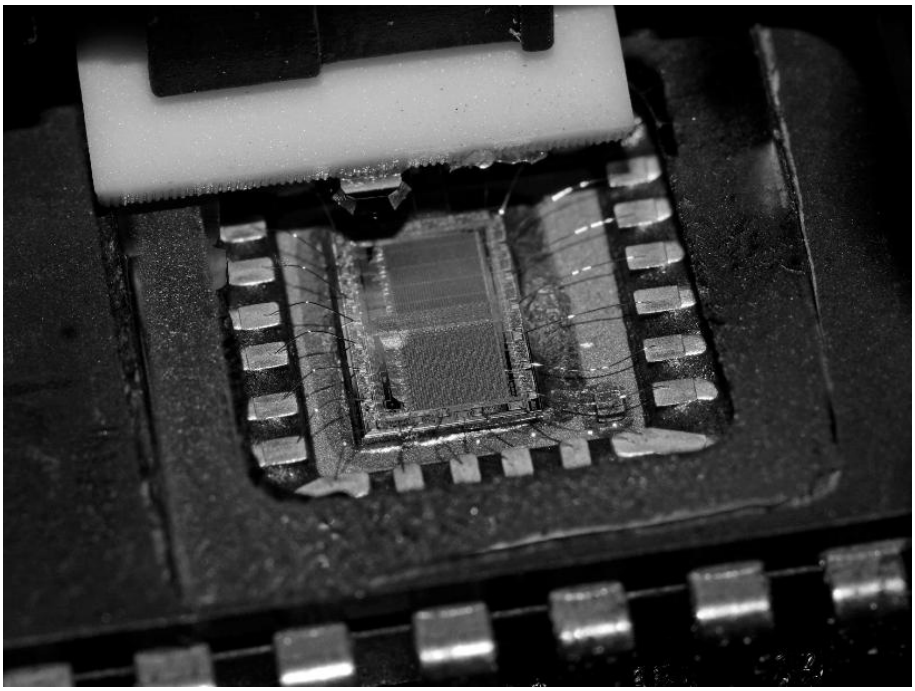

Figure 7. Close-up view of the mounted EPROM chip.

scanner head is tilted up at an extreme angle so that the cantilever chip projects down into the well containing the chip die; this is not an optimal configuration.

Note that Figure 7 shows the EPROM chip in Figures 5 and 6 with its protective quartz window removed. The remainder of the packaging is still intact.

In order to investigate whether or not additional processing would facilitate atomic force microscopy, the top plate of the packaging was removed by cleaving it with a straight sharp blade. This enabled the microscope to be placed in a less contorted posture, but it was still not in its normal configuration. However, imaging was possible and atomic force microscope topographs could be taken.

Figure 8 shows an atomic force microscope topograph of the surface of the memory cell array. The image area is $20\,\mu\text{m} \times 20\,\mu\text{m}$ and the total height variation is $4.4\,\mu\text{m}$. The horizontal stripes and deep holes correspond to the bright white address lines seen in the optical image in Figure 5.

The topograph is remarkably clean and stable, although the uncleaned surface of a 1974-vintage EPROM chip was imaged. Moreover, the sur-

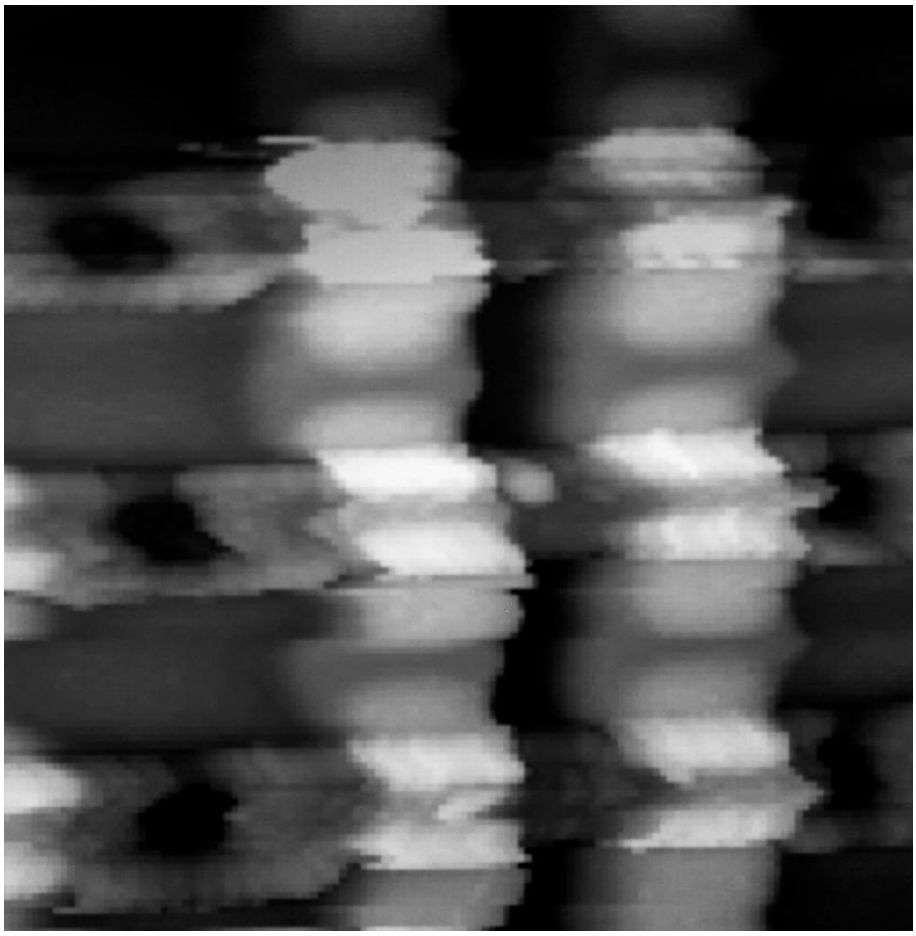

Figure 8. Topograph of the memory cell array in the EPROM chip.

face features can directly be related to those seen in the optical micrograph of the same chip shown in Figure 6. There is a great deal of tip interaction, as can be seen from the sudden jumps and glitches at some points in the image, but given the simplicity of the preparation technique, this is a very encouraging result. Note that although the package had been delidded, all the bond wires were still intact and, in principle, data could be written to the chip.

Experiments involving scanning capacitance microscopy and electrical force microscopy were not conducted. However, it is clear that these techniques would be entirely practicable, although delidding may be more complicated for modern chips with resin packages. In fact, modern chips with low-profile packaging and less surface relief on the die itself

should be easier to investigate because there would much less tip-sample interaction.

7. Conclusions

Atomic force microscopy has already been used to investigate the structures of memory devices and to conduct detailed failure analyses of memory cell structures. However, limited information is available about its application to reading the memory contents of packaged chips. Nevertheless, the published research suggests that atomic force microscopy and related techniques should certainly be applicable to reading memory – the only question is how well.

The initial results presented in this chapter demonstrate that, even without custom sample mounting or modification of the atomic force microscope itself, it is possible to obtain topographic data from a packaged chip using a basic research-grade instrument. If future research demonstrates the feasibility of the technique, it is easy to envision the construction of a custom atomic force microscope that could image integrated circuits *in situ* on their circuit boards. A key aspect of the research would be to perform topside imaging and characterization, avoiding backside polishing and etching and, in principle, maintaining the integrity of the chip as a working device.

The prospects for the future are exciting. Micro-electro-mechanical systems technology and other manufacturing processes that produce smaller, lighter atomic force microscopy structures with higher fundamental resonance would allow for increases in data access rates and crash-free investigations of surfaces with high relief. This would affect the practicability of security and forensic applications discussed in this work. Further development of high-speed electronics and microwave engineering may permit other advances in the surface characterization of semiconductor devices, or they may simply make measurements easier, cheaper and more reliable.

From the point of view of forensic investigations, atomic force microscopy has a number of advantages: it is minimally invasive; it may be performed in a wide variety of environments; and it can be used to image almost any kind of sample. The problems in performing atomic force microscopy investigations of working memory chips are mostly practical, but are of sufficient severity to deter casual investigations. Whatever the future may bring in terms of instruments and their capabilities, one thing is clear – sample preparation techniques will always be of the utmost importance.

References

[1] S. Axelsson, A Preliminary Attempt to Apply Detection and Estimation Theory to Intrusion Detection, Technical Report 00-4, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 2000.

[2] E. Biham and A. Shamir, Differential fault analysis of secret key cryptosystems, *Proceedings of the Seventeenth Annual International Cryptology Conference*, pp. 513–525, 1997.

[3] G. Binnig, C. Quate and C. Gerber, Atomic force microscope, *Physical Review Letters*, vol. 56, pp. 930–933, 1986.

[4] G. Binnig and H. Rohrer, Scanning tunneling microscopy, *Helvetica Physica Acta*, vol. 55, pp. 726–735, 1982.

[5] Bruker, Innova, Billerica, Massachusetts (`www.bruker.com/products/surface-and-dimensional-analysis/atomic-force-microscopes/innova/overview.html`), 2019.

[6] D. Chiang, P. Lei, F. Zhang and R. Barrowcliff, Dynamic EFM spectroscopy studies on electric force gradients of IrO_2 nanorod arrays, *Nanotechnology*, vol. 16(3), pp. S35–S40, 2005.

[7] C. De Nardi, R. Desplats, P. Perdu, C. Guerin, J. Gauffier and T. Amundsen, Direct measurements of charge in floating gate transistor channels of flash memories using scanning capacitance microscopy, *Proceedings of the Thirty-Second International Symposium on Testing and Failure Analysis*, pp. 86–93, 2006.

[8] S. Garfinkel, Digital forensics research: The next 10 years, *Digital Investigation*, vol. 7(S), S64–S73, 2010.

[9] M. Green, Why Can't Apple Decrypt Your iPhone, *A Few Thoughts on Cryptography Engineering Blog*, October 4, 2014.

[10] J. Halderman, S. Schoen, N. Heninger, W. Clarkson, W. Paul, J. Calandrino, A. Feldman, J. Appelbaum and E. Felten, Lest we remember: Cold-boot attacks on encryption keys, *Communications of the ACM*, vol. 52(5), pp. 91–98, 2009.

[11] J. Kim, D. Son, M. Lee, C. Song, J. Song, J. Koo and D. Kim, A wearable multiplexed silicon nonvolatile memory array using nanocrystal charge confinement, *Science Advances*, vol. 2(1), article no. e1501101, 2016.

[12] S. Kinney, *Trusted Platform Module Basics: Using TPM in Embedded Systems*, Newnes, Burlington, Massachusetts, 2006.

[13] P. Kocher, J. Jaffe and B. Jun, Differential power analysis, *Proceedings of the Nineteenth Annual International Cryptology Conference*, pp. 388–397, 1999.

[14] D. Konopinski, Forensic Applications of Atomic Force Microscopy, Doctoral Dissertation, Department of Electronic and Electrical Engineering, University College London, London, United Kingdom, 2013.

[15] K. Lai, W. Kundhikanjana, H. Peng, Y. Cui, M. Kelly and Z. Shen, Tapping mode microwave impedance microscopy, *Review of Scientific Instruments*, vol. 80(4), 043707, 2009.

[16] M. Maroufi, A. Fowler, A. Bazaei and S. Moheimani, High-stroke silicon-on-insulator MEMS nanopositioner: Control design for non-raster scan atomic force microscopy, *Review of Scientific Instruments*, vol. 86(2), 023705, 2015.

[17] I. Mayergoyz and C. Tse, *Spin-Stand Microscopy of Hard Disk Data*, Elsevier, Oxford, United Kingdom, 2007.

[18] J. Pineda, G. Pascual, B. Kim and K. Lee, Electrical Characterization of Semiconductor Device Using SCM and SKPM Imaging, Application Note #8, Park Systems, Santa Clara, California, 2017.

[19] M. Ranum, Thinking about firewalls, *Proceedings of the Second International Conference on Systems and Network Security and Management*, 1993.

[20] J. Rushby, A trusted computing base for embedded systems, *Proceedings of the Seventh Department of Defense/National Bureau of Standards Computer Security Conference*, pp. 294–311, 1984.

[21] S. Skorobogatov and R. Anderson, Optical fault induction attacks, *Proceedings of the Fourth International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 2–12, 2002.

[22] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, Upper Saddle River, New Jersey, 2010.

[23] D. von Oheimb, Information flow control revisited: Noninfluence = noninterference + nonleakage, *Proceedings of the Ninth European Symposium on Research in Computer Security*, pp. 225–243, 2004.

[24] A. Waksman and S. Sethumadhavan, Tamper evident microprocessors, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 173–188, 2010.