Data recovery from damaged electronic memory devices

D I Konopinski†, A J Kenyon†

† Department of Electrical and Electronic Engineering, University College London

Abstract: High value crime involving mobile phones sometimes require examination of highly damaged, possibly exploded devices, currently beyond the capabilities of existing methods. In the pursuit of a forensically sound method to examine damaged memory devices we are investigating a number of techniques to access and analyse samples. Backside processing involving lapping steps, followed by a BOE / TMAH etch is used to access the underside of the bare die, allowing scanning probe techniques, such as Scanning Kelvin Probe Microscopy (SKPM), to examine the charges held on individual floating gate transistors. Despite various remaining challenges and possible techniques to be investigated, this methodology is proving promising for the development of a viable forensic tool.

1. Introduction

The GSM mobile phone network is the largest in the world, with 80% of the worldwide mobile connections and currently approaching 3.5 billion users in over 219 countries [1]. With such widespread implementation it comes as no surprise that this system is widely used in criminal activities. The examination and analysis of mobile telecommunications equipment has subsequently become a vital aid to law enforcement agencies in the forensic investigation of crime.

Information gathered from a mobile telephone system can give an investigator crucial insight into a criminal's actions, contacts and whereabouts. It is vital that any data recovered from the system must be done so with a forensically sound method, i.e. with minimal risk to the data itself [2]. This evidence can be easily gathered from network providers, given the identification of the subscriber via one of the SIM card identity numbers. However, this SIM identification is not always available.

Mobile phones have been used recently in a number of terrorist bomb attacks, either for communication with the bomber, or wired up as detonators to be set off through the built-in alarm clock [3] or by dialling in from elsewhere. An FBI warning in May 2003 about the use of cell phones in terrorism stated that the modifications needed to turn a phone into a trigger were "relatively minor". A typical method of disposal of evidence on mobile phones and SIM cards involves burning them. Despite the physical damage sustained through burning or explosion, data stored on the SIM or handset memory modules may survive such events and the ability to examine this evidence could help identify the owner, last active location, contacts, or calls made and received, providing vital evidence to investigators of these incidents.

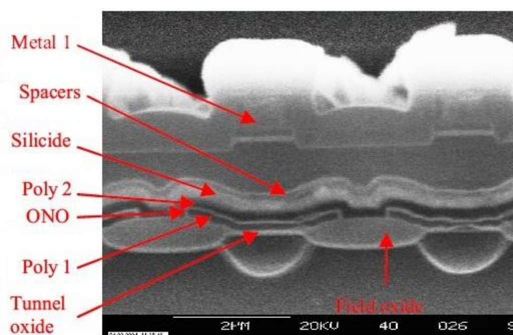

Figure 1: SEM cross-sectional image of an EEPROM device [11]

2. Electronic Memory Data Storage

A mobile phone SIM card is a type of smart card containing a processor and non-volatile memory used as a storage device for user/subscriber-related data, much like that found in an electronic entry card or a 'chip and pin' card. The non-volatile memory in question is EEPROM / Flash memory, widely used among various devices to store software code and data in a microcontroller.

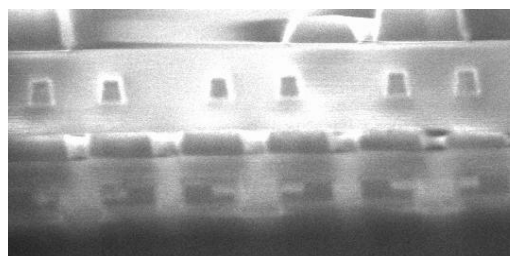

Figure 2: SEM image taken from a FIB crossbeam system showing a cross section through a SIM card die (20µm wide image)

These forms of electronic memory are incredibly robust and reliable due to the physical structure of the floating gate transistors (FGTs) used to store the charge. Data bits are retained in the form of charge stored inside floating poly-silicon gates (POLY 1, Figure 1) within the FGTs. These floating gates are isolated on all sides by protective oxide/nitride layers, thus retaining charge for long periods even while there is no power to the device. The thinnest part of the oxide is the tunnel oxide layer through which electrons tunnel during programming/erasing functions. To ensure data integrity it is vital to keep the tunnel oxide layer intact and able to retain charge, thus incidentally preserving evidence. Figure 1 shows a

scanning electron microscope (SEM) cross-section of an EEPROM, outlining the different layers in the transistor. Figure 2 shows a SEM image of the pairs of floating gate and access transistors taken on a Focused Ion Beam (FIB) crossbeam system in what would be a 90° orientation of Figure 1.

3. Proposed Data Recovery Methodology

This investigation can be thought of as a linear process much like failure analysis; presented with a (possibly) damaged SIM card we need to start by gaining access to the chip itself for examination. Thus, the first step is to develop a solution for the decapsulation of SIM card chips. Various techniques are being explored to assess their limitations and viability within an industry standard solution. Given that a real world scenario would present us with burned, possibly shock damaged cards, various well defined methods need to be in place to expose the chip for forensic examination without destroying evidence. Samples that are relatively undamaged can be rewired in a probe station, allowing for standard forensic electronic data recovery techniques to examine the content of the SIM.

Where chips have been damaged beyond simple rewiring, we will be exploring various scanning probe techniques to measure the stored charge beneath the gate oxide layer without harming data integrity, and thus developing a forensically sound method for data retrieval. SKPM is among the possible AFM techniques we are investigating to read the charge in the floating gates. Following scanning probe analysis, the recovered bit stream must then be returned into a sequenced byte order to read out the contents of the SIM.

For these scanning probe techniques it is necessary to have direct access to the floating gate oxides; unfortunately a topside approach is extremely difficult due to the number of different layers deposited. The alternative and somewhat simpler approach is to target the backside of the wafer, removing bulk silicon through lapping and polishing steps, followed by highly selective chemical etch.

3.1. Sample Preparation

Beginning with decapsulation, many techniques already exist in the field of failure analysis to remove the encapsulating material from an IC to expose the die, ranging from dropping red fuming nitric acid onto the die [4] [5] to much safer solvent-soak recipes [6]. For SIM cards in particular we found that a relatively safe and effective method to remove the majority of the encapsulant involves first cutting away the PVC card (see Figure 3, bottom) then finally soaking the encapsulated chip in a vial of acetone for around 72 hours.

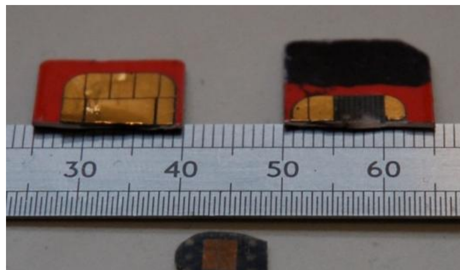

Figure 3: A broken SIM card (top) and an encapsulated chip of the same generation (bottom)

The acetone is absorbed slowly over this period and causes a swelling of the encapsulating material, forming a bubble-like protrusion directly over the die which can then be carefully sliced open, allowing the material to be removed with tweezers, exposing the die. A small amount of material may remain in deep surface features on the topside of the die, but for the purposes of this investigation this is sufficient. To further clean the die, for failure analysis or other related work, a single drop of warm nitric acid should be adequate to remove any remaining encapsulating material while not endangering connections present on the surface.

The die must now be re-encapsulated in an epoxy moulding compound to protect the edges and topside circuitry during the aggressive lapping and TMAH etching processes. Without adequate protection for the sides, the die is destroyed as TMAH laterally etches through it. A suitable epoxy must be chosen and should be thoroughly tested as different materials, methods and curing times produce vastly different results. Silke Liebert conducted such tests on a variety of epoxies at Philips in Zurich, Switzerland and produced a concise report [7] of the problems faced and results. For an epoxy to be suitable for use in backside analysis it must have demonstrated a high resistance to 25% TMAH solution at 105°C. It must also perform well at protecting the sides of the die during lapping, i.e. the epoxy material must have a similar hardness as the silicon. It was discovered that highly viscous epoxies used for cold encapsulation form bubbles and voids at the chip edges, thus allowing TMAH to 'underetch' the die, destroying the sample. Swelling was also investigated as the epoxy can expand when heated, leaving the die edges unprotected. One hot-encapsulation resin was found to be particularly well suited for the task: Powdered EME-7320AR from Sumito Bakelite Co., Ltd., Japan.

3.2. Backside Processing

Once the die is safely encapsulated within a suitable epoxy, lapping can begin. Despite the small size of the dies and their delicate nature, this step is showing promise starting with lapping steps as low as P1200 grit paper (15μm) for removing the majority of the silicon, then moving up to P2500 grit paper (8.4μm) to clean up the surface. This physical removal is completed with polishing steps using 3μm and 1μm diamond pastes.

Following the polishing step, a short dip in a Buffered Oxide Etch (BOE) solution is required to remove the native oxide layer in preparation for the TMAH etch. This is a premixed solution consisting of 40% ammonium fluoride ($[NH_4]F$) in water and 49% hydrogen fluoride (HF) in water in a ratio of 6:1 by volume. This results in an etch rate of SiO_2 of approximately 2nm/s at 25°C.

Silicon dioxide reacts with HF to form hexafluorosilicate ions (SiF_6^{2-}), see Equation (1).

$$SiO_2 + 6HF \rightarrow SiF_6^{2-} + 2H^+ + 2H_2O \quad (1)$$

Ammonium fluoride acts as both a buffer to maintain HF concentration, see Equation (2), and as a source of ammonium ions to form ammonium hexafluorosilicate ($[NH_4]_2SiF_6$), which readily dissolves into the solution, see Equation (3).

$$2[NH_4]F + 2H^+ \rightarrow 2[NH_4]^+ + 2HF \quad (2)$$

$$2[NH_4]^+ + SiF_6^{2-} \rightarrow [NH_4]_2SiF_6 \quad (3)$$

Etching silicon with ammonium hydroxide works well; however, at the higher temperatures required to improve the etch rate this would rapidly evaporate from solution. Thus it is common practice in semiconductor processing to use a variant whereby the ammonium hydroxide is ballasted with a less volatile organic - tetramethylammonium hydroxide (TMAH) or choline hydroxide (2-Hydroxyethyl trimethylammonium hydroxide) are commonly used silicon etchants. For this investigation we have thus far used TMAH to etch silicon.

Silicon dioxide is used as a masking material for TMAH due to its 4000:1 Si:SiO_2 selectivity; it is possible to achieve an etch rate of 600nm/min on silicon, but 0.15nm/min etching the oxide. Thus, to achieve a uniform backside etch it is vital to allow a sufficient BOE dip to remove any native oxide layer present on the underside of the chip. This high selectivity is vital for our purposes as one of our aims is to keep as much of the gate oxide layer intact as possible to maximise charge retention times, thus lowering the risk to the data. A 5nm gate oxide layer left intact will prevent the effects of charge leakage from altering data for around 30,000 years [8].

Various recipes for a TMAH silicon etch are possible [9] [10] [11], among them a solution of 80ml of TMAH solution (25% TMAH in water) and 20ml isopropyl alcohol to enhance the anisotropy of the etch process, at 85°C. The TMAH etch is typically carried out for 60-90 minutes; at 40 minutes and every subsequent 5 minutes the sample should be checked for etch completeness.

After the BOE dip it is imperative to wash the sample clean of any chemical residues by repeatedly washing a minimum of 4-5 times with fresh DI water. After the TMAH etch, cleaning is carried out in a similar fashion and it is recommended to finish cleaning with successive ultrasonic baths of acetone, isopropanol and DI water. It should be noted that TMAH residues will obstruct AFM electrical mode charge measurements at the floating gate interfaces [12].

3.3. Scanning Probe Microscopy

Among electrical AFM techniques, SKPM is proving promising and is thus far our first choice in examining the floating gate transistors. Combining the high spatial resolution typical of electrical AFM techniques with a high sensitivity to surface potentials make this technique an ideal candidate for examining the backside of a processed die. SKPM measures the surface work function of a material by applying an external voltage to balance the contact potential difference. Like Electric Force Microscopy (EFM), SKPM takes two successive scans across a sample; the first scan is a non-contact scan of the surface topography, then the cantilever is raised 10-100nm off the surface and a second surface potential scan takes place. Using the results from the first scan it is possible to achieve a constant distance above any topographical features for the second scan.

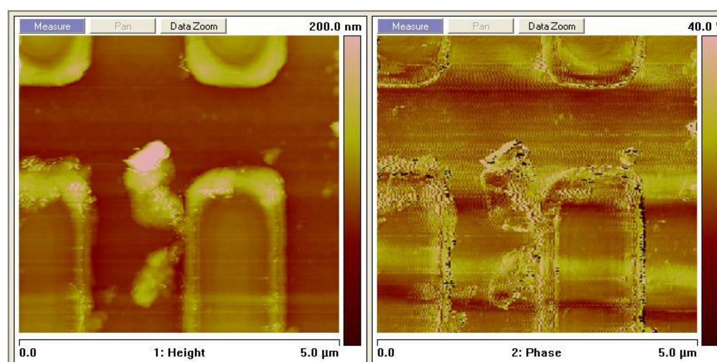

Figure 4: EFM scan of topography (left) and phase (right)

Figure 4 shows a dual EFM scan of both the topography of a sample and the phase image created by the lift scan. Figure 5 shows an SKPM dual scan, in this case the right hand side image shows the surface potential. Both of these techniques are clearly capable of picking up sub-surface features invisible to topography scans, however, SKPM has thus far proven itself to be a more suitable method for examining potential differences within the surface.

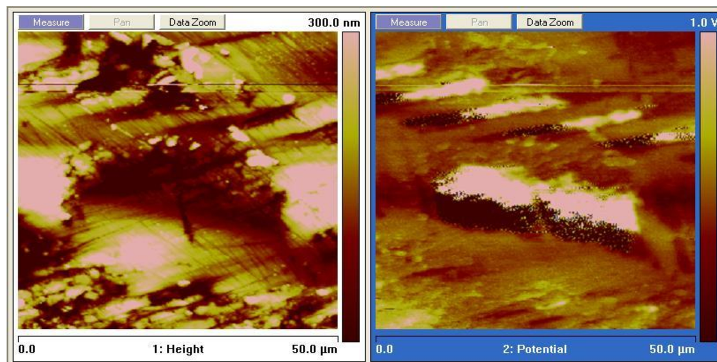

Figure 5: SKPM scan of topography (left) and surface potential (right)

4. Conclusion

Various issues have been tackled thus far in this investigation, including chemical etch recipes, decapsulation methods and initial choices of electrical AFM modes to read data. While these are by no means the only challenges facing the development of a viable method, and the choices thus far made are certainly not set in stone, the methods discussed in this paper give the most likely direction for our route of inquiry to develop a forensically sound method to retrieve data from damaged EEPROM devices.

Acknowledgments

I would like to thank: Steve Hudziak & Kevin Lee at the Electronic & Electrical Engineering Department, UCL; Steve Etienne at the London Centre for Nanotechnology, UCL; Ben Jones at the Experimental Techniques Centre, Brunel University; Jacob Irwin & John Proudlock at the Forensic Science Service.

References

[1] GSM Association. (2009, July) GSM Association - GSM World. [Online]. Accessed 30th July 2009. http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm

[2] Svein Yngvar Willasen, "Forensics and the GSM mobile telephone system," *International Journal of Digital Evidence*, vol. 2, no. 1, 2003.

[3] Jim Boulden. (2004, April) CNN International. [Online]. Accessed 30th July 2009. http://edition.cnn.com/2004/TECH/04/04/mobile.terror/index.html

[4] Y Y Chew, K H Siek, and W M Yee, "Novel Backside Sample Preparation Processes for Advanced CMOS Integrated Circuits Failure Analysis," in *7th IPFA*, Singapore, 1999, pp. 119-122.

[5] Michael Ruprecht, Guenther Benstetter, and Doug Hunt, "A review of ULSI failure analysis techniques for DRAMs. Part II: Defect isolation and visualization," *Microelectronics Reliability*, vol. 43, no. 1, pp. 17-41, September 2002.

[6] Crownhill Mobile Forensics. (2006) 3g Forensics. [Online]. Accessed 30th July 2009. http://www.crownhillmobile.com/DePOT.htm

[7] Silke Liebert, "Encapsulation of naked dies for bulk silicon etching with TMAH," *Microelectronics Reliability*, vol. 42, pp. 1939-1944, May 2002.

[8] D Ielmini, A S Spinelli, and A L Lacaita, "Recent developments on Flash memory reliability," *Microelectronic Engineering*, vol. 80, pp. 321-328, 2005.

[9] Christophe De Nardi, Romain Desplats, Phillippe Perdu, Félix Beaudoin, and Jean Luc Gauffier, "EEPROM Failure Analysis Methodology: Can Programmed Charges Be Measured Directly by Electrical Techniques of Scanning Probe Microscopy?," in *31st International Symposium for Testing and Failure Analysis*, San Jose, 2005, pp. 256-261.

[10] Teh Tict Eng, Hnin Ei Lwin, P Muthu, and J M Chin, "Backside Deprocessing Technique & Its Novel Fault Isolation Application," in *12th IPFA*, Singapore, 2005, pp. 110-113.

[11] Silke Liebert, "Failure Analysis from the Back Side of a Die," in *26th International Symposium for Testing and Failure Analysis*, 2000, pp. 187-194.

[12] Christophe De Nardi, Romain Desplats, Philippe Perdu, Félix Beaudoin, and Jean Luc Gauffier, "Oxide charge measurements in EEPROM devices," *Microelectronics Reliability*, vol. 45, no. 9-11, pp. 1514-1519, September-November 2005.