B.J. Jones and A.J. Kenyon, *"Retention of data in heat-damaged SIM cards and potential recovery methods"*
Forensic Science International (2007)
Archive Version. Definitive version available at DOI: http://dx.doi.org/10.1016/j.forsciint.2007.10.007

Retention of data in heat-damaged SIM cards and potential recovery methods

B. J. Jones[1,2,*] and A. J. Kenyon[2]

1. Experimental Techniques Centre, Brunel University, Uxbridge UB8 3PH

2. UCL Electronic & Electrical Engineering, Torrington Place, London, WC1E 7JE

Examination of various SIM cards and smart card devices indicates that data may be retained in SIM card memory structures even after heating to temperatures up to 450°C, which the National Institute of Standards and Technology (NIST) has determined to be approximately the maximum average sustained temperature at desk height in a house fire. However, in many cases, and certainly for temperatures greater than 450°C, the SIM card chip has suffered structural or mechanical damage that renders simple probing or rewiring ineffective. Nevertheless, this has not necessarily affected the data, which is stored as charge in floating gates, and alternative methods for directly accessing the stored charge may be applicable.

Keywords: SIM card; mobile phone; fire; data recovery; scanning probe microscopy

* *Corresponding Author:* B.J. Jones b.j.jones@physics.org +44 (0)1895 265409

1. Introduction

The ubiquity of mobile phone use in the general public can be an asset in crime scene investigations. Many criminals and victims of crime will be carrying mobile phones, each with a unique Subscriber Identity Module (SIM) card. However, in some cases such as road traffic accidents and building fires, mobile phones may be significantly damaged, either mechanically or by high temperatures. In addition, mobile phones have been used recently in a number of terrorist bomb attacks, both as detonators [1-3] and for communication [4]. Data may be retained in even highly damaged phones and an ability to read this data could help identify the owner, place of purchase, last active location, or calls made and received [5, 6], which could provide vital assistance to investigators of these incidents [7]. Reading data from the memory of damaged SIM cards, and similar devices such as credit cards and some types of ID cards, will therefore assist in the identification of both victims of incidents and perpetrators of crimes.

During forensic investigations, the most valuable part of an embedded system, such as might be found in a smart-card or a mobile phone SIM card, is the memory - in particular the non-volatile re-writable memory. This is usually implemented as an erasable electrically programmable read-only memory (EEPROM). Conventionally, data from the EEPROM are read using an interface on the same chip as the EEPROM, and a number of forensically sound techniques exist to study data in undamaged SIM cards [8]. In cases where the chip package has been damaged, and making contact via the attached interface is not feasible, data can be extracted by making electrical contacts on the surface of the chip itself. However, this practice is becoming more and more difficult for a number of reasons, such as the likelihood of the chip being locked by a personal identification number (PIN) and the manufacturer's unlocking code (PUK) cannot be obtained, and, in particular, because of the high likelihood of the chip being damaged during criminal activities, by fire, or during extraction. Figure 1 shows damage to a SIM card recovered from a waste-paper fire.

Data are held in a typical EEPROM memory in the form of individual data bits (0 or 1) each consisting of charge stored on a floating polycrystalline silicon gate embedded in a silicon dioxide layer, shown schematically in figure 2. The floating gate is electrically isolated top and bottom by an oxide layer; the tunnel oxide is of thickness around 10nm, this is sufficiently thin to allow Fowler-Nordheim tunnelling of electrons from the gate to the source and vice-versa. Charge, typically 10^3 to 10^5 electrons, is introduced onto the floating gate by applying a high voltage (typically 12V) to a second control gate placed over the floating gate, and charge is removed by grounding the control gate and applying a positive voltage to the source [9, 10, 11]. The presence of charge on the floating gate modifies the conduction between a diffused source and drain in the underlying silicon substrate, and determining whether the source and drain are electrically isolated or connected by a high resistance conduction path allows discrimination between logical 1 and 0. Once in the floating gate, charge is held there by the large potential barrier formed by the surrounding oxide. The quality of the oxide is of paramount importance in producing reliable memory cells with long data retention times, and modern EEPROMs are capable of holding charge for several decades. There is much research and development into different architectures and materials to produce faster, higher-density non-volatile memories [11-14] – however, these devices are currently used for digital photography and video capability, where these attributes are of primary importance [14].

Increased operating or storage temperature of EEPROMs and similar devices will cause a reduction in the data retention capabilities of the device, and recent research outlines a number of models for high temperature data loss [15] in addition to novel high-level devices for increased reliability in high operating temperatures [16]. However, damage by heat or fracture may cause a SIM card or similar device to become unreadable via the interface or through direct probing of electrical contacts or bit and word lines, but will not have necessarily compromised the stored data. This work aims to ascertain if data is retained within a heat damaged SIM card or smart card, independently of the accessibility of this data via conventional methods. We then outline alternative data extraction methodologies.

2. Experimental

Samples of SIM cards currently and recently in use were collected from members of the public in Ireland, Sweden and the UK. New SIM cards and similar smartcards were supplied by, or purchased from, networks or other distributors. The sample set therefore represents a range of manufacturers including Infineon and ST Microelectronics, packaged by Gemplus and ACS.

SIM cards, pre-programmed by the network with IMSI number etc, were further programmed using a converted Motorola phone to enter sample data such as numbers dialled, memorised contacts and text messages (it is worth noting that, depending on the phone model, size of memory, fraction of memory available etc, data may be stored either in the phone memory or on the SIM card). Blank SIM cards and SIM-type smart cards were programmed with sample data via an ACR38-1080 interface manufactured by Advanced Card Systems Ltd, or a similar SIM card reader device, connected to a PC.

Damage to SIM cards can occur by mechanical means or when the cards are heated (such as in house fire or explosion) and further damage can be caused by the processing of the device prior to probing for data, such as the removal of epoxy and other packaging materials by the use of heated nitric or sulphuric acid [17]. Decapsulation of SIM card chip, via any method, can cause mechanical damage to the chip, or reveal or exacerbate existing damage. Even a low level of damage can render the chip unreadable via connection to a SIM card reader or simple probe station.

For this study we minimised the possibility of damage to the circuitry, which would render rewiring or probing ineffective. Before any heating occurred, the SIM cards were stripped of plastic moulding to expose the chip, which is further encased by a protective epoxy or plastic - the type varies depending on the model - and protects the chip and wiring that connect to the SIM card interface. This casing can be removed with acid treatment as outlined above. In some instances, the casing can be removed mechanically or by heating to temperatures not exceeding 160^{o}C - some of the encasing materials become pliable as the temperature is moderately increased, and can

be more easily removed. Note that several different types of epoxy, plastic and other materials may be used in chip packaging; consequently, different protocols must be developed for the optimal removal of encapsulation, depending on the SIM card type.

Chips were detached from the interface, extracted from the casing and then heated in ambient air to a range of temperatures. Chips were held at their maximum temperature for approximately ten minutes and then cooled by removing from the heat source. Following heating, the chips were attached to an interface pad using conductive paint, and rewired to the interface using a Kulicke & Soffa 4523 wire/ribbon bonder. The remounted chips were then read via the SIM card reader attached to mobile phone or PC.

3. Results and Discussion

3.1 Heat damage to SIM cards

In this experiment, twelve decapsulated chips were studied: six heated to approximately 180^{o}C, five to approximately 450^{o}C and one to approximately 650^{o}C. Of those that suffered no mechanical damage (assessed by light microscopy with 2x to 20x magnification) all those heated to temperatures up to 180^{o}C could be read after rewiring, showing no loss of data. One SIM card heated to approximately 450^{o}C was rewired and fleetingly operated to retrieve data; however, most chips experiencing this temperature suffered damage rendering data reading by rewiring impossible; figure 3a shows an example of a SIM card chip heated to 450^{o}C. Above this temperature significant damage occurs which renders data retrieval by rewiring impossible. Figure 3b shows a SIM card chip heated to 650^{o}C, showing heat induced material damage and mechanical fracture.

The experimental arrangement is deliberately artificial; all the material surrounding the chip is removed before heating, and therefore we present an idealised situation. Nevertheless, through this we show that the stored data can be read in instances where the chip is not mechanically damaged, and therefore propose that the data itself, stored as charge on floating gates, is not compromised by the heating process. In real

situations, of course, a chip that has been exposed to such temperatures may also be mechanically damaged, and the data may not be retrieved by simple probing or rewiring - but the data itself remains uncompromised and can possibly be read using other techniques.

This experiment demonstrates that the SIM card in this work retained data after heating to 450^{o}C. This is not necessarily indicative of all SIM card models, due to possible differences in the electronic architecture, which may affect data retention times. However, the experimental results are supported by data published by manufacturers. Most memory device manufacturers provide nominal data retention times for operation at room temperature. In some cases, this can be extrapolated to operation times at different temperatures, using a variety of models. For example, data retention times for the Texas Instruments flash memory used in the MSP430F microcontroller families are of the order of 100 years at room temperature; however, extrapolating information provided by the manufacturer using the Arrhenius equation [18], indicates that data loss is accelerated at higher temperatures, leading to a data retention time of about twelve days at 180^{o}C, decreasing to approximately one hour at 450^{o}C. As temperatures reach 750^{o}C the retention time has reduced to a few minutes. This is a simple extrapolation, and some mechanisms for charge loss, such as a stress-induced leakage current, or trap-assisted transport, may vary differently with temperature. It nevertheless provides approximate figures and illustrates the trend of data retention with temperature.

These experimental and manufacturers' temperature figures compare favourably to the temperatures reported by Putorti and McElroy [19] in their experiment on a full scale house fire, fuelled by household furniture and accelerated with unleaded petrol and oil. This experiment showed that the temperature experienced in such a fire varies with location within the house, and increases significantly with height. The maximum temperature in the floor area, up to 15cm from the floor, is 166^{o}C and temperatures here are in fact only maintained above 100^{o}C for 90 seconds – indicating that phones in these locations will not suffer data loss due to heating effects. At 0.76m above the floor, approximately desk height, the temperature is sustained at an average of 450^{o}C. From the extrapolated figures it can be seen that data retention will

only become an issue for semiconductor memories that experience this temperature for approximately an hour or longer. The maximum temperature obtained in the house is 738^{o}C; this is obtained briefly, however, and temperatures are only sustained above 650^{o}C for a maximum of 42 seconds, this duration occurring at a height of 1.98m above floor level. This is still less time than the extrapolated data retention time at this temperature; however, consideration should also be given to any additional exposure of the device to temperatures in the range 350^{o}C – 650^{o}C and the combined effects of this and the brief period above 650^{o}C could in some cases result in temperature-induced data loss.

It is worth noting that the temperatures given above are maxima and the house fire temperature is considerably reduced away from the source of ignition and highly combustible furnishings. For example, in an adjacent room to that which experienced the maximum temperatures stated above, the desk height temperature does not exceed 260^{o}C and the floor area does not reach temperatures above 50^{o}C [19], both comfortably allowing sustained data retention. Other work [20] shows greater variation in recorded temperatures, due to various materials present, but data follows the trends outlined above.

3.2 Data Reading Techniques

Now that we have established experimentally that data may still be present in semiconductor memories that have been exposed to high temperatures, such as those encountered in domestic fires, we turn our attention to the feasibility of reading this data from chips that have been exposed to elevated temperatures and have suffered mechanical damage. An important point to note is that it is not always necessary to read all of the data held on a SIM card. In many cases, only a very small fraction of the data is necessary – for example, the IMSI number can yield valuable information linking the card and phone to a specific person and a particular location.

A range of techniques exists for monitoring the operation of embedded microprocessors in order to access protected data or programmes during programme execution. Such techniques range from the non-invasive (probing the external

connections to a processor and monitoring power consumption during operation) to the highly invasive (such as fault induction [21]). The former group are referred to as *side channel attacks*, and rely on the ability to monitor unintended outcomes of processor operation; for example, it is possible to measure charge movement within processors using microscopic probes that detect magnetic fields around tracks (so-called electromagnetic analysis, EMA). A very simple method probes the time taken to perform certain arithmetic operations depending on the size of the data being operated on; however, as an elementary fraud countermeasure, current generations of smart cards are designed so that the time taken for different processes is the same.

Recent techniques addressing the problem of protecting systems using a combination of cryptographic and physical protection systems have relied on the un-accessed memory being secure [22], and concentrate on protecting the processor during operation.

The emphasis is thus on protection of operating processors and preventing attacks aimed at determining the contents of secure memory via ascertaining the structure and operation of the processor, rather than those directly aimed at detecting static charge in the EEPROM cells.

Most of these techniques require the removal of passivation, metallisation, and control gate from the EEPROM. Well-established methods exist to achieve this; however, removal of the upper layers can cause degradation of the charge retention characteristics of the target chip before enough material has been removed to allow probing methods access to read any charge on the floating gate [23]. In addition, and potentially more seriously, in-built chip security measures may detect such an attack; for example, optical sensors and capacitive sensors to detect the passivation layer are sometimes built into systems to prevent successful reverse engineering [17, 24].

An alternative to these methods is to access the memory via etching the backside of the wafer and apply electrical scanning probe microscopy (SPM) methods such as scanning capacitance microscopy (SCM) or scanning Kelvin probe microscopy

(SKPM) to read the charge in individual floating gates, each corresponding to one bit. This has been used successfully in the past as a failure analysis technique for space science applications [23], and has the advantages of not requiring the upper circuitry to remain intact - thereby circumnavigating some security countermeasures - and is operable even if only fragments of the chip are available. This may, therefore, be a useful technique to detect the data that the current study shows is retained as charge even in damaged chips. However, there are considerable drawbacks in such techniques, including the very slow read speed, damage to cells during the preparation process, leakage of charge following preparation [25] which compromises the integrity of any data retained – and, lastly, the descrambling of the binary contents of the memory array into meaningful data. Such a method may therefore be useful, after development, for extracting the small amounts of data from a SIM card, but would be unsuitable for large capacity devices, such as Flash memory drives.

4. Conclusions

We have shown that data may be retained in EEPROM memory devices such as SIM card memory, even when the SIM card chip is subjected to a temperature up to ~450^{o}C. This is approximately the maximum average sustained desk height temperature in a house fire, and is significantly above the maximum floor temperature of 166^{o}C [19]. In some cases the data is retrievable by rewiring the chip or by making direct contact to the chip surface. However, in the majority of cases, chips heated to 450^{o}C or above will suffer additional damage to the top surface or circuitry, or experience some mechanical damage. In these cases, although the data is retained in the memory, the data cannot be read by rewiring or with a conventional probe station, and an alternative technique, such as direct probing of the stored charge, needs to be employed to access the retained data.

Acknowledgements

This work is funded by the Engineering and Physical Sciences Research Council of the UK (grant EP/C523369/1), as part of the "Think Crime!" Initiative, and by the Royal Society (2007/R1/R27011). We acknowledge the assistance and guidance of

Dr Silvia Valussi of The Forensic Science Service®. Thanks go to Lucy Atabey of Virgin Mobile Telecoms Ltd for provision of samples, and to Kevin Lee of the department of Electronic & Electrical Engineering, UCL, for assistance with rewiring.

References

[1] The Guardian, London, UK *"58 Die in car bombing in Iraqi market"* (7 May 2005) p.13

[2] Newsday, NY, USA *"Cell phones jury-rigged to detonate bombs"* http://www.globalsecurity.org/org/news/2004/040315-cellphones-bombs.htm (15 Mar 2004)

[3] CNN, Cable News Network, Atlanta, GA, USA *"Bombs were Spanish-made explosives"* http://www.cnn.com/2004/WORLD/europe/03/12/spain.blasts/ (13 Mar 2004)

[4] BBC News, London, UK *"London bomber called accomplices"* http://news.bbc.co.uk/1/hi/uk/4181454.stm (24 August 2005)

[5] E. Philips *Science and Justice* **42** (2002) 225

[6] S.Y. Willassen "Forensics and the GSM mobile telephone system" *Intl. Journal of Digital Evidence* **2** (2003) 1

[7] G. Pugh "Delivery and Development of Forensic Services in the Metropolitan Police Service" *Science in Parliament* **62** (2005) whit12

[8] B. Mellars "Forensic examination of mobile phones" *Digital Investigation* **1** (2004) 266

[9] S. Haddad, C. Chang, A. Wang, J. Bustillo, J. Lien, T. Montalvo and M. Van Buskirk *IEEE Electron. Dev. Lett.* **11** (1990) 514

[10] A. Chimenton and P. Olivo *Microelectron. Reliab.* **45** (2005) 1478

[11] A. Regnier, R. Laffont, R. Borchahar and J.M. Mirabel *J. Non-Cryst. Sol.* **351** (2005) 1906

[12] R.S. Edelstien, C. Cork, E. Alorei, N Vofsy and Y. Roizin *Microelectron. Eng.* **72** (2004) 421

[13] B.J. Jones and R.C. Barklie *Microelectron. Eng.* **80** (2005) 714

[14] Samsung press release "*SAMSUNG First to Mass Produce 16Gb NAND Flash Memory"* (2007) April 29

[15] C-S Pan, K Wu, D Chin, G Sery and J Kiely *IEEE Electron Dev. Lett.*, **12** (1991) 506

[16] S.G.M. Richter, D. Kirsten, D.M. Nuernbergk and S.B. Richter "A Novel Low Leakage EEPROM Cell for Application in an Extended Temperature Range (−40°C Up to 225°C)" in "Science and Technology of Semiconductor-On-Insulator Structures and Devices Operating in a Harsh Environment" *Nato Science Series* **185** (2005) 285

[17] M. Kuhn and O. Kömmerling *Information Security Technical Report* **4** (1999) 28

[18] Peter Forstner "MSP430 Flash Memory Characteristics" *Texas Instruments Application Report* SLAA334 (2006)

[19] A.D. Putorti Jr and J. McElroy "*Full-scale House Fire Experiment for InterFIRE VR*" US Dept. of Commerce, National Institute of Standards and Technology Report of Test FR4009 (2000)

[20] J. Deans "Recovery of fingerprints from fire scenes and associated evidence" *Science and Justice* **46** (2006) 153

[21] S. Skorobogatov and R. Anderson, "Optical fault induction attacks", in: Cryptographic Hardware and Embedded Systems (CHES 2002) *Lecture Notes in Comp. Sci.* **2523** (2003) 2

[22] S. Micali and L. Reyzin, "Physically Observable Cryptography", *Lect. Notes in Comp. Sci.* **2951** (2004) 278

[23] C. De Nardi, R. Desplats, P. Perdu, F. Beaudoin and J-L. Gauffier *Microelectronics Reliability* **45** (2005) 1514

[24] O. Kömmerling and M. Kuhn "Design Principles for Tamper-Resistant Smartcard Processors" in: Proc of the USENIX Workshop on Smartcard Technology (1999)

[25] D. Ielmini, A.S. Spinelli and A.L. Lacaita "Recent developments in Flash memory reliability" *Microelectronic Engineering* **80** (2005) 321

Figures

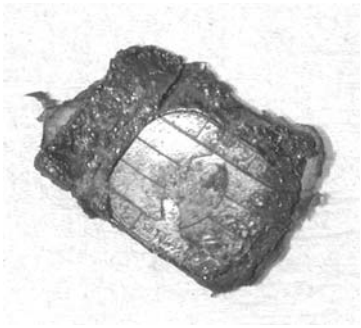

Figure 1. SIM Card recovered from waste-paper fire

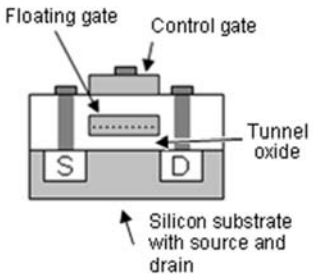

Figure 2. Cross-sectional schematic of a basic EEPROM. The poly-Si control gate and metallisation lie above the poly-Si floating gate, which is isolated in an oxide.

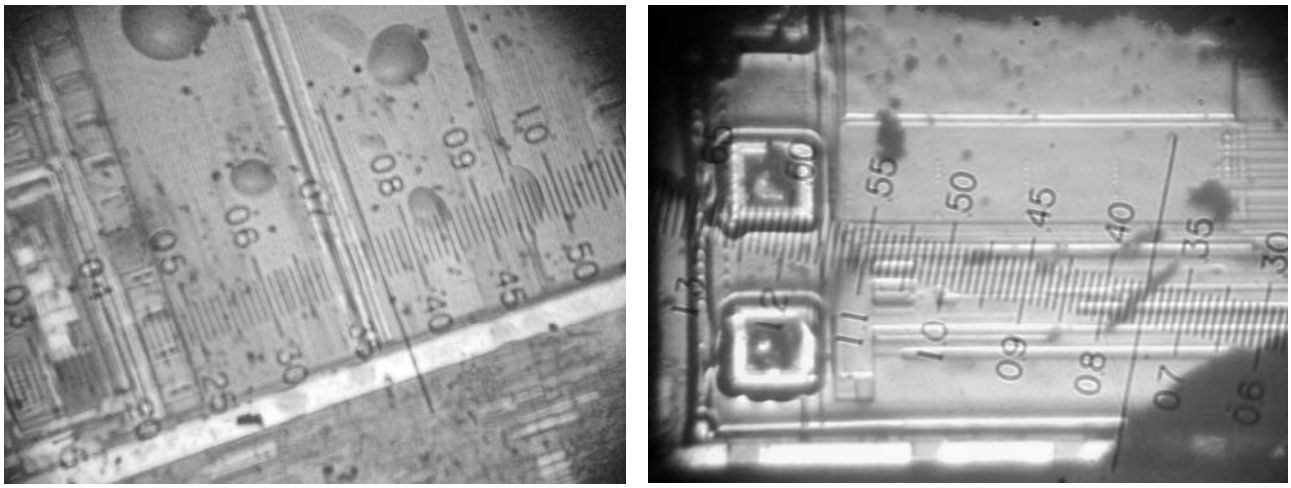

Figure 3. a) and b) Optical micrographs showing damage to SIM card chips by exposure to temperatures of a) ~450^{o}C and b) ~650^{o}C;