*Technical Report*

UCAM-CL-TR-536
ISSN 1476-2986

Number 536

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

# Low temperature data remanence in static RAM

Sergei Skorobogatov

June 2002

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom
phone +44 1223 763500

*http://www.cl.cam.ac.uk/*

Technical reports published by the University of Cambridge
Computer Laboratory are freely available via the Internet:

*http://www.cl.cam.ac.uk/TechReports/*

Series editor: Markus Kuhn

ISSN 1476-2986

# Low Temperature Data Remanence in Static RAM

Sergei Skorobogatov
*University of Cambridge Computer Laboratory*
sps32@cl.cam.ac.uk

## Abstract

Security processors typically store secret key material in static RAM, from which power is removed if the device is tampered with. It is commonly believed that, at temperatures below −20°C, the contents of SRAM can be 'frozen'; therefore, many devices treat temperatures below this threshold as tampering events. We have done some experiments to establish the temperature dependency of data retention time in modern SRAM devices. Our experiments show that the conventional wisdom no longer holds.

## 1. Introduction

Security engineers are interested in the period of time for which a static RAM device will retain data once the power has been removed. The reason for this is as follows. Many products do cryptographic and other security-related computations using secret keys or other variables that the equipment's operator must not be able to read out or alter. The usual solution is for the secret data to be kept in volatile memory inside a tamper-sensing enclosure. On detection of a tampering event, the volatile memory chips are powered down or even shorted to ground. If the data retention time exceeds the time required by an opponent to open the device and power up the memory, then the protection mechanisms can be defeated [1][2][3].

In the 1980s, it was realised that low temperatures can increase the data retention time of SRAM to many seconds or even minutes. With the devices available at that time, it was found that increased data retention started about −20°C and increased as temperature fell further [2]. Some devices are therefore designed with temperature sensors; any drop below −20°C is treated as a tampering event and results in immediate memory zeroisation [4][5]. We set out to repeat this work. Our goal was to find whether the memory devices available in the year 2000 exhibit the same behaviour.

Another important thing to keep in mind is that security information could be restored even if part of the memory is corrupted. Suppose an attacker has correctly restored only $m$ = 115 bits of an $n$ = 128 bits long secure key, or 90% of the information. Then he will have to search through $n!/(m!(n–m)!)$ = $128!/(115!13!) = 2.12\times10^{17} \sim 2^{58}$ possible keys. Having 10,000 computers, each performing 1 billion key-search operations per second, the attacker will spend only 6 hours to search through all possible keys. If only 80% of information or 103 bits of a 128-bit secure key are known, than an attacker will need $2.51\times10^{26} \sim 2^{88}$ searches. Having even 100 times the capability, the attacker will spend more than a million years searching for the key. So to be sure that symmetric 128-bit keys cannot be retrieved from memory, it should be left without power for the time necessary to corrupt 20% or more of the cells. If error correction for key data is used, this value should be increased correspondingly. In our experiments, we assumed that no error correction was used.

## 2. Experimental Method

We built a special circuit board for testing static RAM chips. All signals were controlled by a PIC16F877 microcontroller working at 4MHz, which was connected via a RS-232 interface to a computer for programming the necessary modes and downloading information. The power supply line of the SRAM chip was controlled by a CMOS switch (MAX314). We also had an LCD display and two buttons for hand controlling the experiments. For supplying the board, we used a standard

9V AC adaptor and a 78L05 linear regulator to provide 5V for the ICs. For convenient insertion and extraction of SRAM chips, we put a lock/eject socket on to the board. Also, we put an external connector for testing SRAM chips inside a freezer. In this case, we used a flat cable with an IC socket at the end.

For temperature control, we used an LM135H temperature sensor, which operates from −55°C to +150°C with ±1°C precision, and provides an output voltage directly proportional to the absolute temperature at +10mV/K. For temperature monitoring, we used a standard digital multimeter.

For temperatures from +25°C down to 0°C, we used Peltier elements. For lower temperatures, we used a domestic freezer in conjunction with Peltier elements.

Each SRAM chip was tested under two conditions – with the power supply pin shorted to the ground after power-off, and with it left floating. The test algorithm was the following:

- Set the necessary temperature;
- Apply power supply;
- Write test pattern (all 0's or all 1's);
- Remove power supply;
- Wait the required time;
- Switch power on again;
- Read out data from memory;
- Calculate how many bits retain their state.

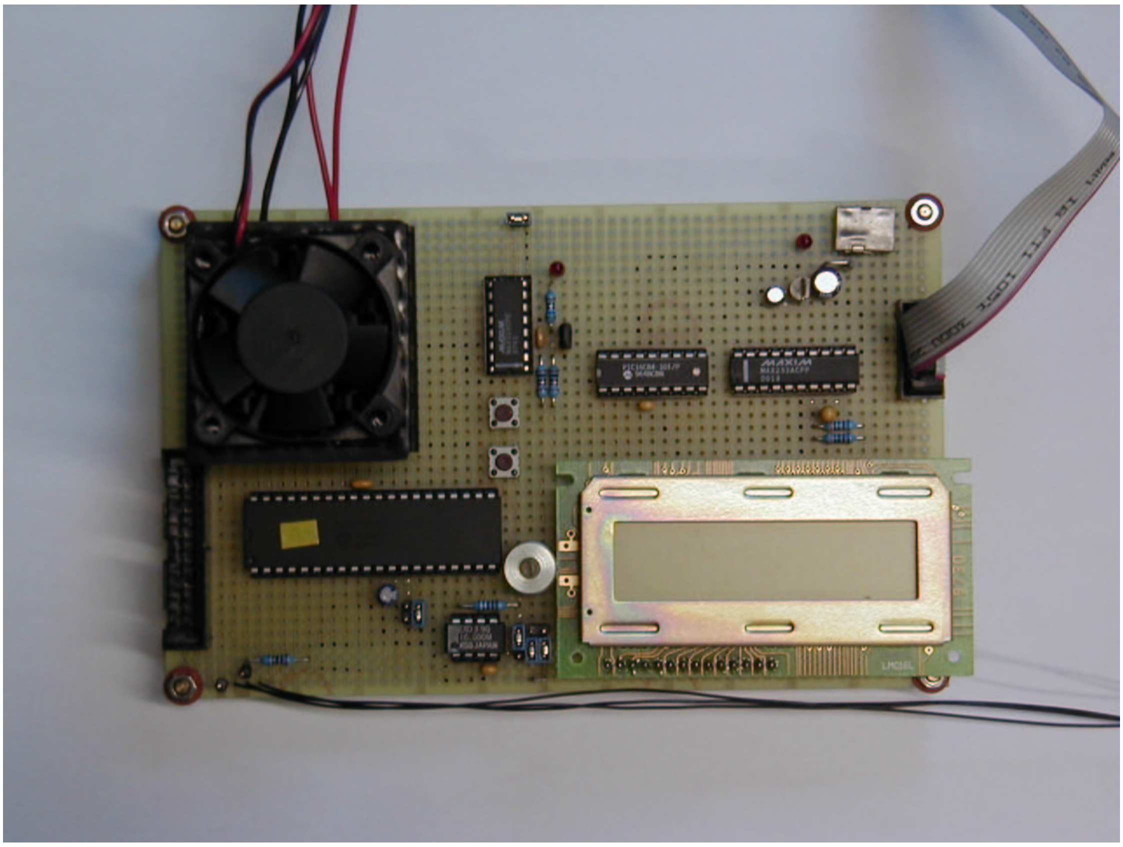
Eight different SRAM samples were tested at different temperatures. All SRAM samples were bought from a semiconductor distributor (Farnell). Here is the list of the SRAM chips we tested, with their date of production:

1. Dallas DS2064-200, 1999
2. GoldStar GM76C88AL-15, 1995
3. Hyundai HY6264AP-10LL, 1996
4. Hyundai HY62256BLP-70, 1998
5. NEC D4364C-15, 1987
6. NEC D4364C-15L, 1987
7. Samsung K6T0808C1D-DB70, 2000
8. Toshiba TC5564APL-15, 1989

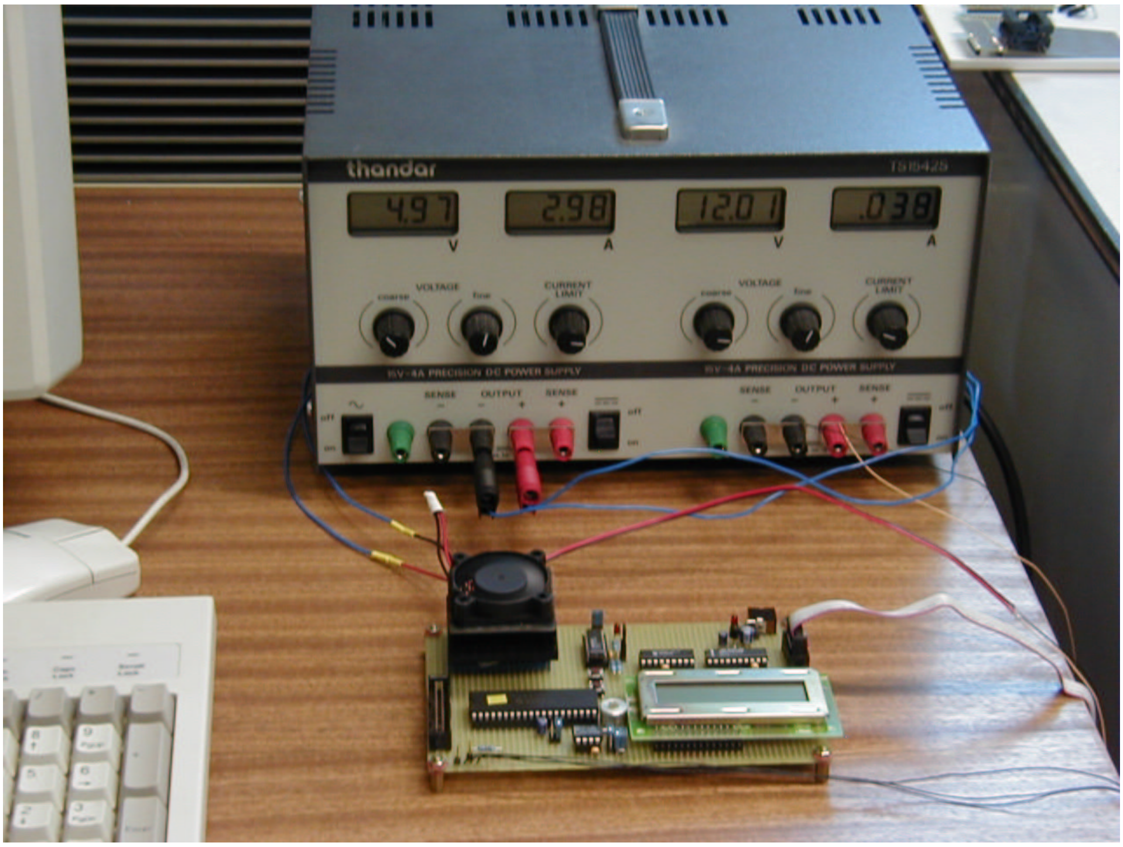
We also measured the power supply current, in non-active mode, for all SRAM samples at room temperature. Because this current is very small, it is not possible to measure it directly with a digital multimeter. To measure this current, we built a circuit board with a MAX4374H current sense amplifier (100×) and a socket for the SRAM chip. As a sensor we used a 10kΩ resistor, so the output voltage on the MAX4374H corresponds to the power supply current with a ratio 1mV per 1nA. The results of these measurements are represented in Table 1.

| **Sample** | **TC5564** | **DS2064** | **K6T0808** | **D4364CL** | **HY6264** | **HY62256** | **GM76C88** | **D4364C** |
|---|---|---|---|---|---|---|---|---|
| **Current** | **1nA** | **2nA** | **9nA** | **319nA** | **357nA** | **384nA** | **1375nA** | **1697nA** |
| **Ret.Time (shorted)** | **3519ms** | **2316ms** | **1366ms** | **65ms** | **34ms** | **65ms** | **20ms** | **12ms** |
| **Ret. Time (floating)** | **13100ms** | **12200ms** | **4611ms** | **206ms** | **67ms** | **206ms** | **63ms** | **37ms** |

An important observation is that the smaller the power consumption of the chip, the longer is its data retention time. We suspect that this will hold even where chips come from the same batch.



Picture 1. Top view of the board.



Picture 2. Side view of the board.

## 3. Results

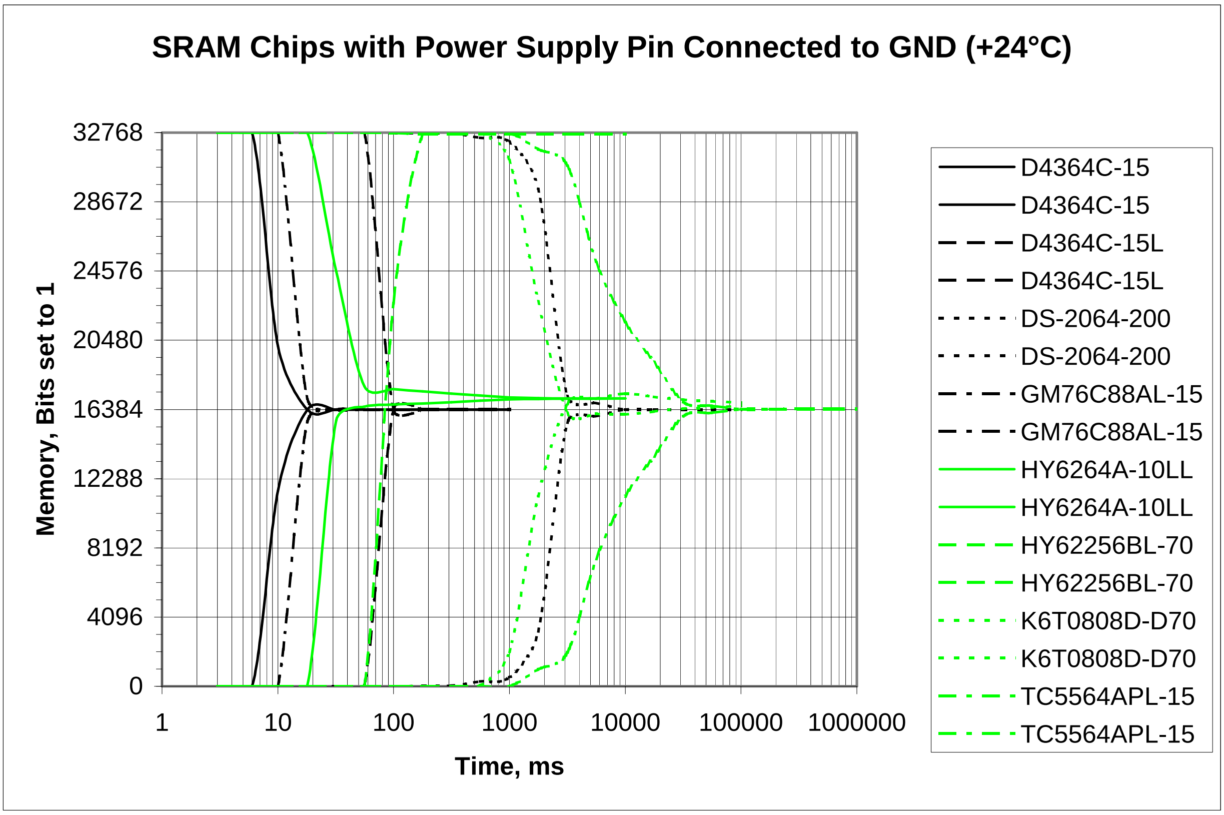


Figure 1. Number of memory bits equal to 1 after switching power off. T = 24°C. Power pin connected to GND.

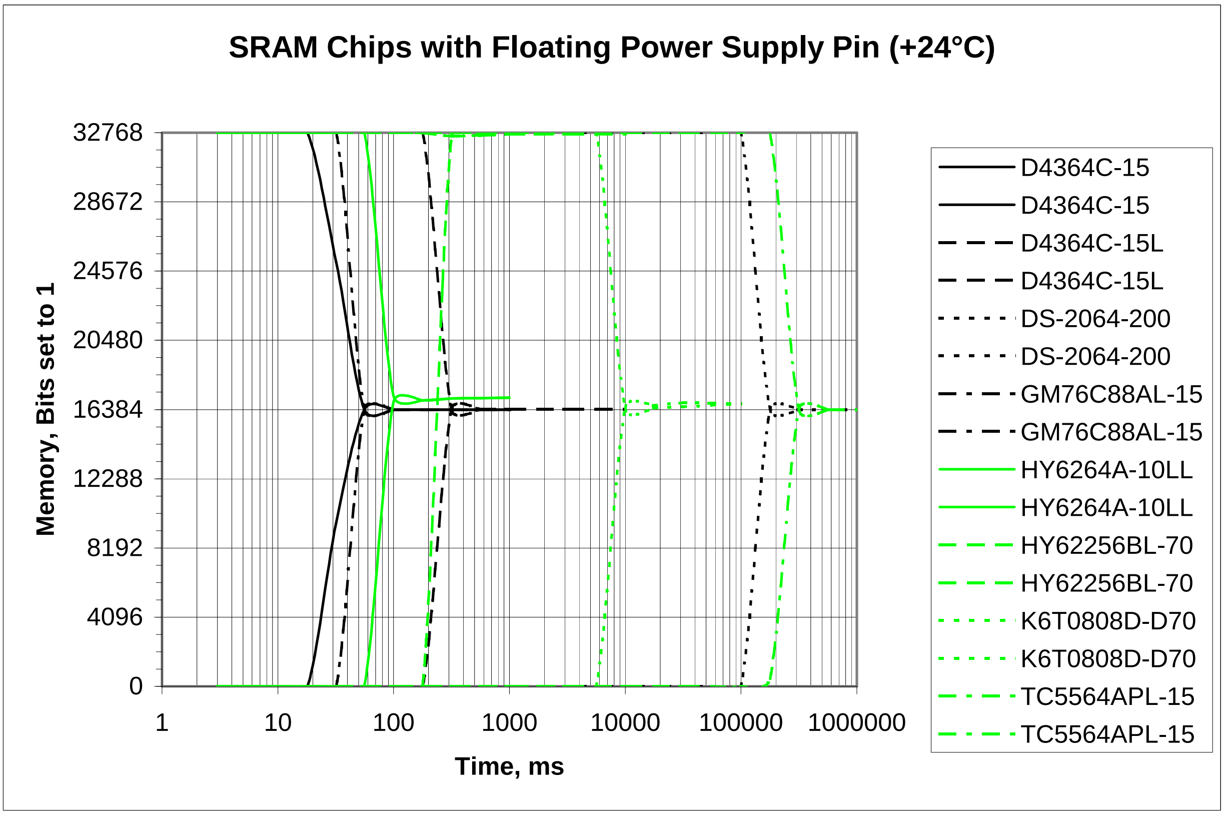


Figure 2. Number of memory bits equal to 1 after disconnecting power. T = 24°C. Power pin left floating.

With the power-supply connected to ground, the data retention time is always less than if the power-supply pin is left floating. Once information loss from an SRAM chip begins, it proceeds quickly.

Comparing the two SRAM chips NEC4364C-15 and NEC4364C-15L (the last one is a low power version) we can note that the low power version has a longer retention time at any temperature. The reverse situation holds with the HY6264A-10LL and HY62256BL-70. The first one is an ultra low power version, but, although the second one is the low power version, it has a longer data retention time, because it was produced later and it was designed using smaller transistors. Thus it consumes less power.

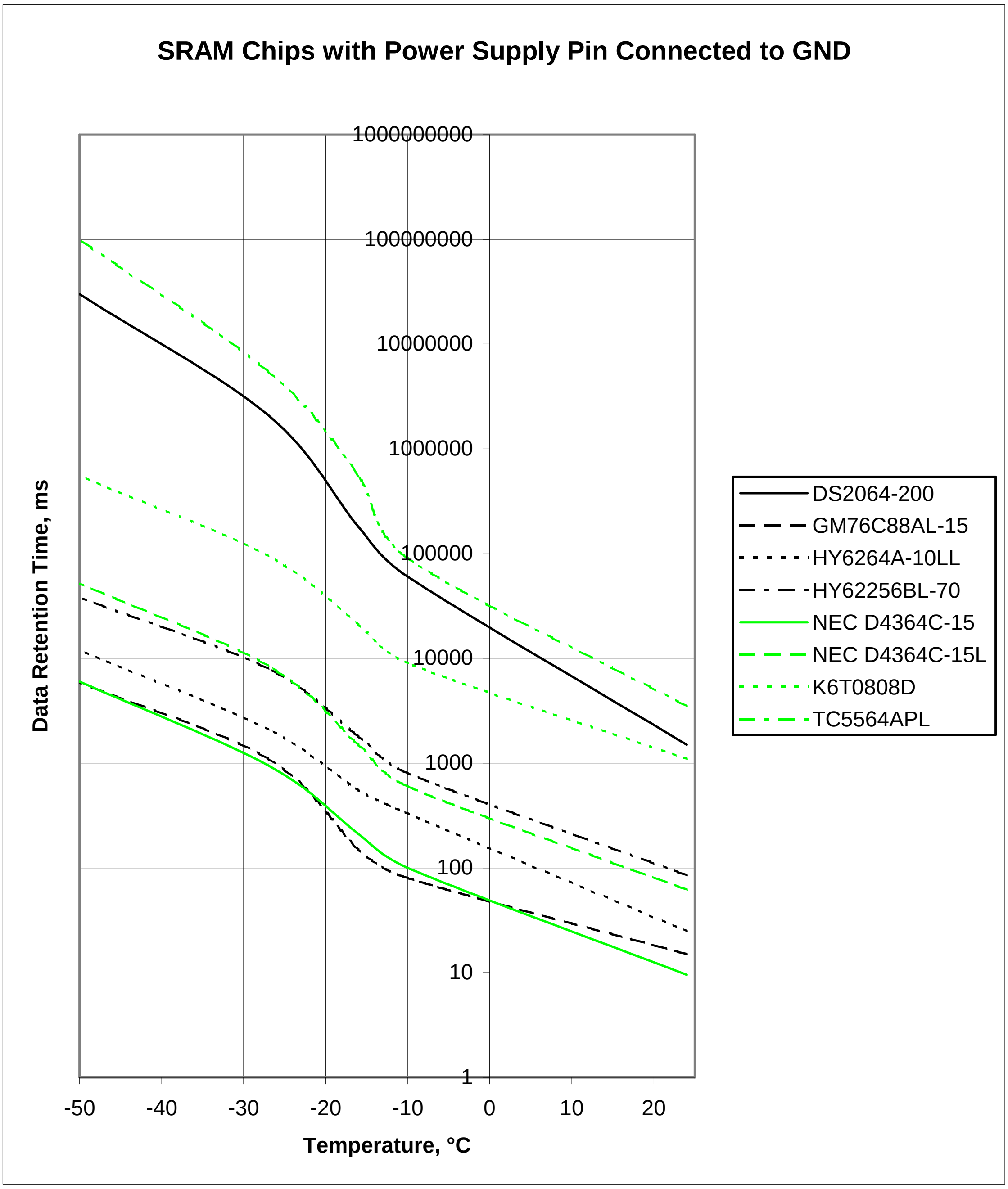


Figure 3. Dependence of data retention time from temperature. Power pin connected to GND.

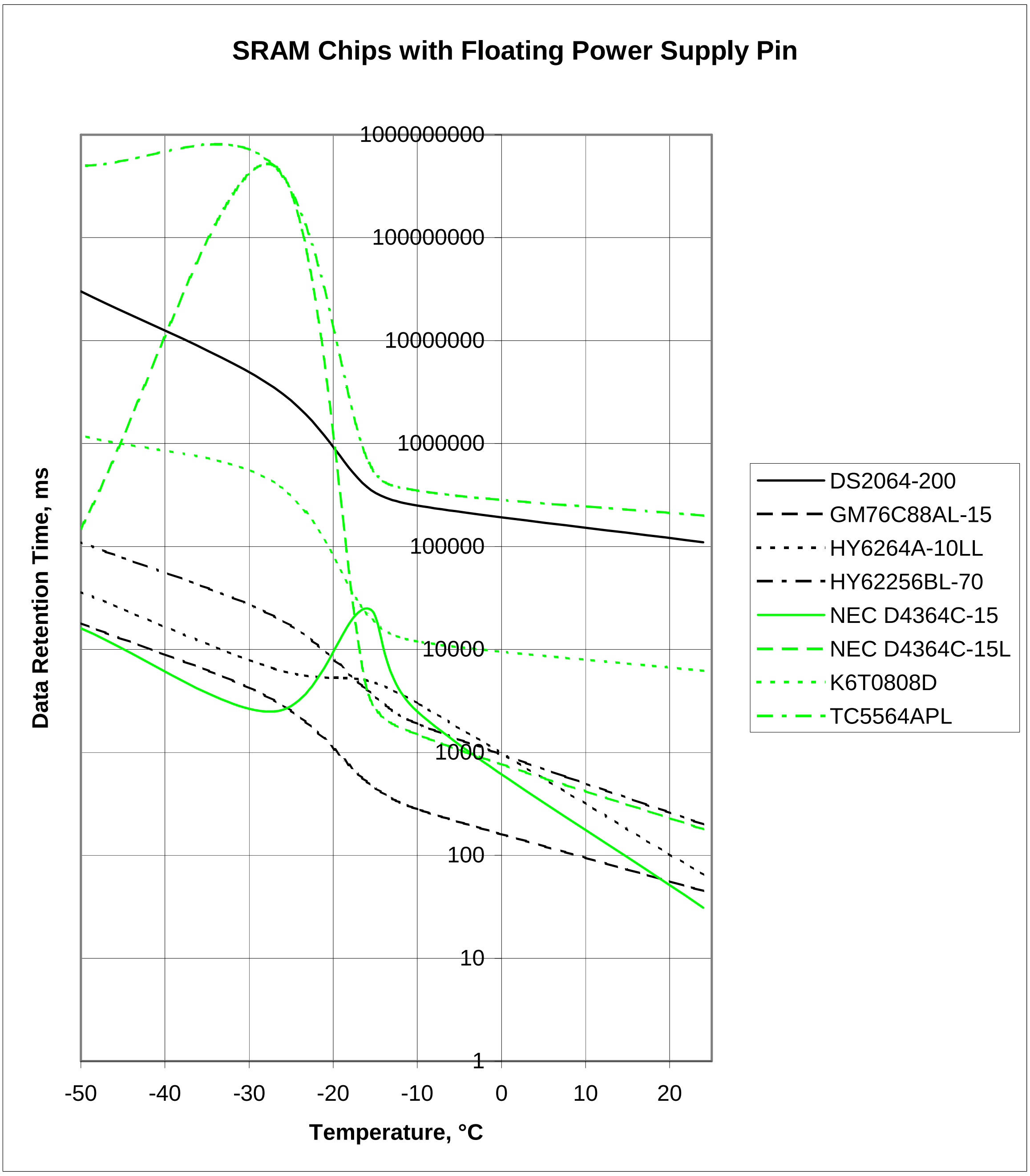


Figure 4. Dependence of data retention time from temperature. Power pin left floating.

## 4. Conclusion

We tested and documented the data retention characteristics of a sample of modern SRAM chips, as a function of temperature. Contrary to the established wisdom, there are several chips that retain data for dangerous periods of time at temperatures above −20°C. The temperature at which 80% of the data are retained for one minute varies widely between devices. Some require cooling to at least −50°C, while others retain data for this period at room temperature. Retention times can be significantly reduced by shorting VCC to ground rather than by leaving it floating. Another unexpected observation is that memory retention time varies not just from one device type to another, but also between devices from the same manufacturer and of the same type but of different subtype or series. Presumably this is because chip makers do not control data retention time as part of their manufacturing quality process. Low power versions of the same chip always seem to have longer retention times. Thus, to build secure processors that reliably erase memory on tampering, it would appear to be vital to test chip samples before use. As this is time-consuming, it will not usually be feasible for each individual device. However, measuring the power consumption of each chip in a batch can give a useful and practical test of inter-device variability.

## References

[1] Peter Gutmann. Secure Deletion of Data from Magnetic and Solid-State Memory, 6th USENIX Security Symposium Proceedings, San Jose, California, July 22–25, 1996

[2] Sean W. Smith, Steve Weingart. Building a High-Performance, Programmable Secure Coprocessor, Computer Networks 31, April 1999, pp. 831–860

[3] Sean W. Smith, Elaine R. Palmer, Steve Weingart. Using a High-Performance, Programmable Secure Coprocessor, Second International Conference on Financial Cryptography, Springer-Verlag LNCS 1465, February 1998

[4] Steve H. Weingart. Physical Security for the μABYSS System, Proceedings of the IEEE Computer Society Conference on Security and Privacy, 1987, pp. 52–58

[5] Steve H. Weingart. Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses, Workshop on Cryptographic Hardware and Embedded Systems (CHES 2000), Springer-Verlag LNCS 1965, pp. 302–317