18 Chip Decapsulation

So far, we've covered a number of vulnerabilities that can be exploited electrically, either through software bugs or through externally triggered fault injection. Many more attacks are possible once the packaging is stripped away, revealing the bare glass of the microchip beneath. In this chapter, we'll cover the chemistry used to open up chips, then a little later we can see examples of firing lasers into them, photographing their mask ROMs, and using ultraviolet light to erase their EEPROM, OTP, or flash memory.

Before we begin, it's important to know a bit about how chips are put inside their packages. Microchips are first manufactured on discs called wafers through a lithography process. Layers are individually placed down and then etched away, with a mask and light exposure controlling what remains and what washes away. At the end, the wafers are sawn apart into individual dice, then tested and sorted.

Those dice that pass testing are placed into a wide variety of packages. Packages with pins, such as dual in-line packages (DIPs) and small outline integrated circuits (SOICs), begin as a metal lead frame. The die is glued to this frame, and pin pads of the die are bonded with microscopically fine wires to the pins of the frame. Epoxy then locks the die and the pins in place, after which the pins are bent into shape.

See Figure 18.1 for two examples. The upper X-ray is the frame of TO92 transistor packages after plastic encapsulation. The lower X-ray is the bare frame of DIP16 before the die is

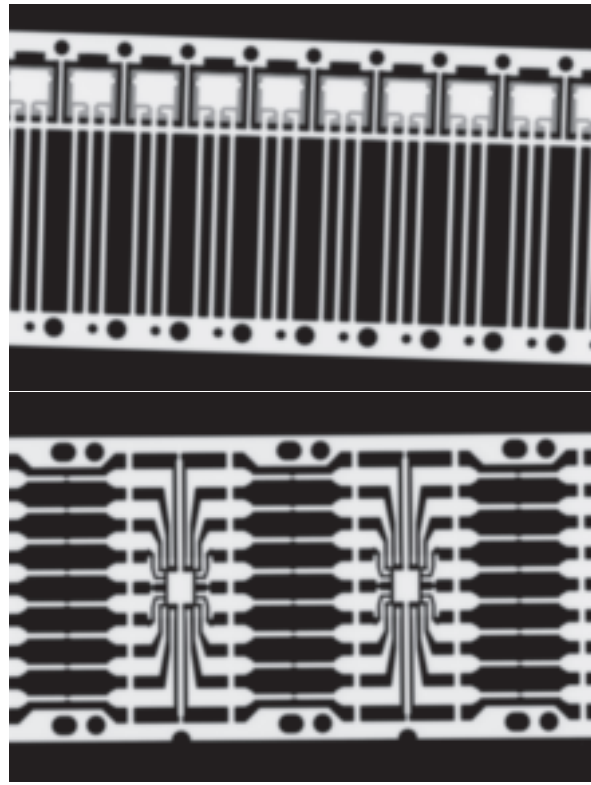

Figure 18.1: TO92 and DIP16 Lead Frames

bonded. After encapsulation, the factor would cut apart the pins of each of these and then bend them into the appropriate shape for distribution.

Things can also be packaged in very different ways. System-in-package (SiP) devices bond multiple dice to a single circuit board, then epoxy the circuit board as if it were a lead frame. Wafer-level chip-scale packaging (WLCSP) places solder balls directly on the die, so that it can be soldered to a circuit board without being encased in epoxy. When this packaging gets in our way, it's time for a trip to the chemistry lab.

Lab Supplies and Equipment

Let's begin with a shopping list. In terms of lab equipment, you will need a fume hood, hotplate, and ultrasonic cleaner. 30 mL, 50 mL, and 100 mL Pyrex beakers will hold the chemicals. Plastic pipettes will move acids from their containers. (Glass pipettes feel cool, but their rubber bulbs tend to petrify and crack.) Also buy some cans of computer duster and some very sharp tweezers.

For safety, you will want a labcoat, gloves, and glasses. Long hair should be tied back, and do not play any games with open footwear unless you want to learn what it's like to walk with acid burns on your toes.

For solvents, you will want acetone and isopropyl alcohol (IPA). I also stock distilled water, which you can buy cheaply as CPAP water. For chemicals, you will want 65% nitric acid (HNO_3) and 98% sulfuric acid (H_2SO_4) to begin with. I suggest holding off on purchasing more exotic chemicals until you are familiar with the bath methods, as some of them are dangerous to your health and difficult to dispose of.

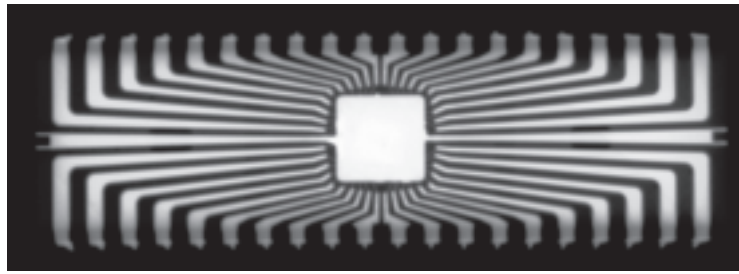

Figure 18.2: X-ray of a DIP40

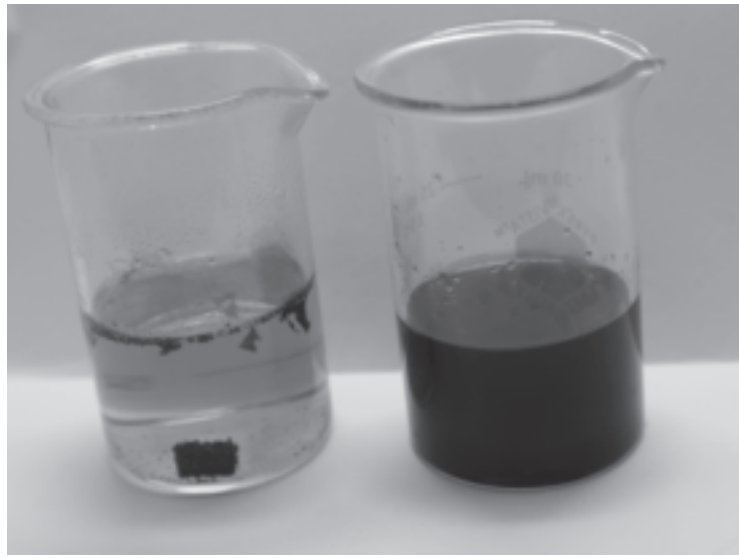

Figure 18.3: HNO_3 and H_2SO_4 Baths

HNO_3 Bath Method

This method is the first that many of us learn, and it is still the most common procedure for casual decapsulation in my lab.

The method works best with surface mount chips, as their package is not much larger than the die. For large packages, such as the DIP40 X-rayed in Figure 18.2, the procedure becomes unbearably slow. Almost all of these chips have the same structure as in the X-ray, with the die mounted between the dead-center pins. A quick cut with a bandsaw can remove the majority of the plastic, reducing the processing time and conserving nitric acid.

Begin by cutting the pins of the CPU to free it from the board, then drop it in a small beaker filled halfway with 65% nitric acid. You'll see faint wisps of green where the acid reacts with the remains of the pins, but we'll need some heat to burn off the plastic.

In heating the nitric acid, you want to make it hot but you do *not* want it to boil. Carefully raise the temperature until you see the reaction begin, but drop it back down when you see bubbles coming from the liquid rather than the chip.

The early reaction might be a little disappointing on your first try, with the liquid turning a very slight green and little more than the silkscreen burning away from the plastic. That is caused by the outer surface of any metal oxidizing against the acid, and it will hang around in that state until the temperature is high enough for the plastic to break down. (Metal here can be the lead frame, the bond wires, or in older chips the exposed top metal layer of the die.) Raise the temperature slowly, so that you don't accidentally boil over the side of the beaker.

When the packaging reacts with nitric acid, small pieces will crumble off as if they came from an Oreo cookie. You need to continue the reaction until the microchip's die and its lead frame

have been freed from their plastic tomb.

The die is attached to the lead frame with glue. Sometimes this glue weakens during decapsulation and the two pieces separate, and sometimes the frame dissolves in the acid. If they don't separate and the frame does not dissolve, you can free the die with a neat chemical trick. Simply add a little distilled water to fresh acid and scratch the lead frame with tweezers. The oxidized surface of the frame is what prevents the acid from hurting the frame. This oxide layer will be broken by the scratch, and the whole frame will dissolve in the dilute acid as the water washes away freshly formed oxides or rust. Metal is best attacked by about 20% nitric acid, and you'll see later in this chapter that the lead frame and bond wires do not dissolve in very strong nitric acid.

Once the die is free, boil it in a clean beaker of distilled water to remove any metal salts, then give it two ultrasonic baths: first in acetone and then again in isopropyl alcohol. The acetone is a lot better at dissolving or breaking up dirt, but this means that there are dirt particles on the chip after the acetone bath, so a second bath of isopropanol will clean the dirt away.

Finally, place the die on the microscope slide while it is still wet, and use the computer duster to lightly blow the alcohol off the surface rather than letting it dry. (If it were to dry, there would be less dirt than with acetone, but there might still be a little to blow away.) Grip it firmly while you do this and use rather little air pressure, as it's a frustrating waste to watch the poor die fly off into the abyss of a dusty laboratory.

H_2SO_4 Bath Method

Rather than 65% nitric acid, you might also want to decap chips with sulfuric acid, either the 98% from a chemical supplier or a lesser grade sold for cleaning drainage pipes. The procedure is largely the same, so in this section I'll focus on the differences.

Nitric acid causes the packaging to crack off and crumble away. This lets you see the progress of the reaction, but it also means that a few crumbs of packaging might remain attached to the glass, where the acetone might not brush them away. Sulfuric acid blackens from heat and it dissolves the packaging into very fine particles, which leaves a much cleaner surface. This comes at the cost of the liquid being absolutely opaque; you will not see your progress until the sample has been removed from the acid.

Aqua Regia for Gold

Plastic DIPs are a hassle, but the techniques earlier in this chapter are sufficient for extracting dice from them. Some low-volume ceramic packages, however, have a gold coating on the frame that prevents sulfuric or nitric acid from freeing the die. As the ceramic itself is impervious to these acids, and the lid is easily desoldered, we might instead take apart the gold with aqua regia to free the die.

Aqua regia is a mixture of hydrochloric and nitric acids, with a molar ratio of three to one: $HNO_3 + 3\,HCl$. The mixture fumes at room temperature, and while it is clear at first, it will quickly turn orange or red as chlorine and nitric oxide fumes dissolve back into the liquid.

I've found that the ratio isn't particularly important for the thin layer that I need to dissolve in order to free the die. It's

sufficient under heat to drip a little nitric acid and a little hydrochloric acid, even if the latter is not particularly strong.

RFNA Drip Method

In past sections, we learned that nitric acid is more corrosive to bond wires and the frame in *lower* concentrations, as water acts as a catalyst to take metal salts away from the metal. We can take advantage of this by dripping very small quantities of red fuming nitric acid (RFNA) to open a pit into the package without damaging the bond wires. The chip remains functional, which is necessary for photovoltaic attacks and probe needles.

RFNA is very strong nitric acid, more than 90% HNO_3 and less than 2% H_2O. This requires special shipping restrictions, as I learned when my order of less than half a liter arrived in a five-gallon bucket strapped to a shipping pallet!

To open a chip, begin by soldering it to a small carrier board with nothing on the opposite side. You'll want to heat it on your hotplate to somewhere above 100 °C.

Elsewhere in your fume hood, but in a location where you will not knock it over, place a few milliliters of cold RFNA in a small beaker. Take a pipette with a very narrow tip, and draw just a tiny bit of acid into the tip. Then draw a small line with the acid in the very center of the package, above the die. After letting it burn for a bit, use pure acetone to wash off the acid and some pieces of the packaging into a very large beaker.

A few notes of caution: do not accidentally use isopropyl alcohol (IPA) or water for cleaning. IPA detonates on contact with RFNA, producing a small popping sound in minute quantities and considerable embarrassment in larger quantities. H_2O will help the nitric acid damage bond wires, and any water or water-bearing chemicals must be strictly avoided for this to succeed.

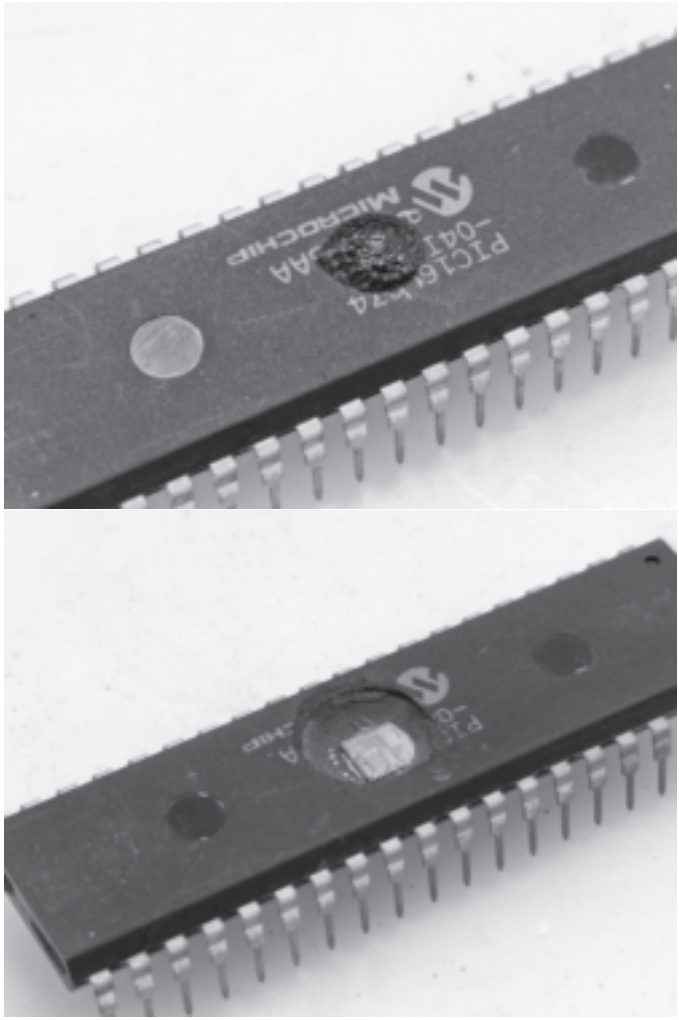

Figure 18.4: RFNA Drip Method on a PIC16LC74

After the first exposure has been made and washed away, carefully inspect the sample. You should see a small trench and the removal of any silkscreen where the acid made contact, and you should not see any corrosion of the package pins or of the carrier PCB. If you find the acid dripping over the side, you are using way too much. The early amounts should be far less than one full drop.

I've warned you to keep the acid in the trench and to keep the trench small, but you do both of these things once or twice to understand why. If the trench grows too wide, pins of the lead frame might break off, taking their bond wires with them. You should also see that acid prefers to soak into the chip where the epoxy has previously been etched away; if the acid spills out of the trench, it will make more of the surface attractive to absorbing acid.

Repeating this procedure will quickly give you a trench that can hold a larger droplet of acid. Do not be tempted to let the acid boil until it is dry, and it's usually a good idea to shorten your exposure times as you get closer to the glass, leaving less residue on the surface. Figure 18.4 shows both an early drop and the final result, with the PIC16LC74 die exposed.

Once the surface is completely exposed and you expect no further droplets of acid, you can safely rinse the chip in distilled water and IPA. Do not do this earlier in the procedure, or the water might damage the bond wires.

Rosin or Colophony

I live in the United States, which to readers in Europe might seem to be an unregulated frontier in which gun-toting hillbillies can privately possess the same chemicals used in industrial failure analysis laboratories. Those readers aren't exactly wrong, but let's take a moment to consider how they might decapsulate chips without nitric or sulfuric acids.

Schobert (2010) describes a technique from Beck (1988) in which pine resin or colophony is used to strip the package away.[1] The package is boiled in pine resin at 350 °C for five or ten minutes to free the die. Of course the resin will solidify as it cools, but dissolving it in acetone will free the die again for photography.

This method is messy, but it is quite cool that decapsulation can be performed with nothing but supplies from beauty and music stores.

Other Techniques

In this chapter, we've learned a number of ways for extracting the glass die from a microchip. Chapter 22 will extend these chemical techniques with delayering and Dash etching, as a means to reveal the diffusion layer and to highlight the difference between P and N silicons. It will also explain how ROM bits can be extracted to ASCII art and rearranged from their physical order into logically ordered bytes suitable for emulation and disassembly.

1. Sadly this passage is not found in the English rewrite, Beck (1998).