Disabling the NES "Lockout Chip" (rev. 0.4 22-Sep-97)

Introduction

This document details a simple modification that you can perform on your Nintendo Entertainment System video game console in order to remove the "lockout chip" protection system.

Why might you want to do this? Well, I can think of a couple of reasons:

- You own unlicensed games which can't be played on your model of NES;
- You own foreign games, and currently have to use a clumsy adapter system. For example, after performing the modification you can use most PAL games on a U.S. console, and use most U.S. games on a PAL console console.

The procedure given here should work for ANY old design NES (i.e., any front-loading model). The new design NES doesn't have a lockout chip anyway.

With the modification, you can play *ALL* PAL games (European, Hong Kong or U.K.) on *ANY* PAL console. However, you can't play all PAL games on a U.S. console, or play all U.S. games on a PAL console. Some games are incompatible with the different display standards. Examples of this are High Speed, Pin Bot (both hang the console), Time Lord, Digger T. Rock, and various other games developed by Rare Ltd. However, the majority of games do work fine.

NOTE: IF YOU KNOW HOW TO CONVERT A PAL NES TO GIVE A 60Hz DISPLAY, PLEASE CONTACT ME! IF THIS IS POSSIBLE, IT WILL ENABLE *ANY* NES GAME TO BE PLAYED ON *ANY* NES, AT THE CORRECT SPEED. Modifications similar to this are easily done on SNES, Master System and Mega Drive/Genesis consoles, but I suspect that the NES would need a new PPU chip.

If you perform this procedure on your console, PLEASE LET ME KNOW WHETHER IT WORKS! I want to update this document so that it's applicable to as many consoles as possible. Please tell me which PCB revision your console has (e.g. NES-CPU-11), the serial number and also the lockout chip number (e.g. "3197A").

I have successfully carried out this procedure on a U.K. model NES, which has PCB revision NES-CPU-11. All unlicensed games that I own, and U.S. and European licensed games work fine. (The unlicensed games which I tried are Action 52, Crystal Mines, Firehawk and Super Adventure Quests.)

This procedure has been reported to work on a U.S. model NES, revision

NES-CPU-11.

If you are interested in the operation of the lockout chip and the NES' history in general, you might like to read David Sheff's excellent book "Game Over", and consult U.S. patents 4,799,635 and/or 5,070,479. Indeed, I obtained the information necessary to carry out this modification from one of these patents.

Background

Before the NES was first released in the U.S.A., Nintendo developed a system for preventing the use of unauthorised software with it. Much counterfeit software had apparently been produced for their Famicom (Family Computer) game system, and Nintendo wanted to avoid this happening for the NES.

Another benefit (to Nintendo, at least) of the system was that legal third-party development was severely hindered. Only Nintendo licensees could buy the lockout chips, one of which was fitted inside every game cartridge. Licensees were apparently charged around US$9 for each chip.

Some companies managed to get around the lockout system and produce their own unlicensed games. Examples of this are Active Enterprises, Codemasters/ Camerica, Color Dreams and Tengen (though Tengen's system was ruled to infringe Nintendo's copyright on the "10NES" program, the program inside the lockout chip). Macronix Inc. filed U.S. patent 5,004,232, which details a method for getting around the lockout.

However, during the life of the NES Nintendo periodically modified the console, meaning that some unlicensed games no longer worked. For example, "Action 52" and "Crystal Mines" do not work on my U.S. NES. If your NES has board revision NES-CPU-11, it will be unable to play these games. Disabling the lockout chip solves this problem.

Nintendo also used the lockout system to provide a "territorial protection". This means that you can't use a U.K. or European game in a U.S. console, for example. At least four different types of lockout chip are used in U.K., European, Hong Kong and U.S. machines. A cartridge with one type of lockout chip is incompatible with a console containing any other type.

How the Lockout System Works

This is a very brief description. Consult Nintendo's patent for detailed information.

Identical chips are fitted to the console and inside every game cartridge. Depending on whether a certain pin (pin 4) of the chip is grounded or at +5V, the chip functions as either a lock or as a key. Inside the console, pin 4 of the lockout chip is at +5V (lock), and inside the game cartridge pin 4 is at 0V (key).

When you switch on the NES, the CPU and PPU are held in a reset state. The two lockout chips talk to each other. Since the chips are identical, they should be saying exactly the same thing at exactly the same time. Each chip compares its output with that of its counterpart. If they match, the lock chip releases the reset state of the console, and the game can start. The two chips still talk to each other, and if the outputs of the two chips ever differ, the lock chip causes the console to repeatedly reset, and the key chip inside the game cartridge may use the chip select lines of the cartridge ROM chips to disable them (though this disabling of the ROMs was probably never done).

The lockout chip is in fact a 4-bit microprocessor with its own internal ROM and RAM. The program in the ROM is called "10NES".

How the Modification Works

This depends on changing the lock device to think that it's actually a key. If both devices are configured to be the same type (i.e., both keys), to quote Nintendo's patent "an unstable state takes place and no operations are performed at all."
This means that the two chips will do nothing. So the console will not be reset, and the key device will not disable the cartridge ROM chips.

To carry out the modification you need to disconnect pin 4 of the lockout chip, and connect this pin to ground (0V) instead. If you do something wrong and the entire pin 4 breaks off, don't worry. This is what happened to me, but the console still works fine. It may not be absolutely necessary to connect pin 4 to 0V; leaving it unconnected may be okay.

When I was thinking about what might be done to defeat the protection system, I came up with three answers. The first is the simplest and is that presented here.

The second is more complicated and works in a different manner. I have not tried this method, so I can't say whether it actually works. Basically, it involves connecting the output of each chip to that chip's input. So each chip would 'talk to itself'. Since the input will always be the same as the output, the chip will think that its counterpart is of the right type, and will not reset the machine.

The third method involves disconnecting the 4MHz clock from the lockout chip in the console and the line that leads to the lockout chip clock pin in the cartridge. This may well work - if there is no clock, both devices should be halted, and thus will not be able to do anything.

Performing the Modification

You will need the following:

- A crosshead screwdriver suitable for opening the NES case and removing the screws inside;
- A very sharp, very small knife, pair of scissors or similar to cut the IC pin - a two-sided implement (e.g. scissors) is preferable to a knife;

· A soldering iron and solder, and optionally some desoldering braid;
· A short length of thin insulated wire, with the ends stripped of insulation - 2cm is enough.

When removing screws, make sure you remember which type goes in which hole!

Here are step-by-step instructions:

1. Remove the six screws from the base of your NES and lift off the upper part of the case.

2. Remove the seven screws which attach the upper metal shielding to the PCB, and remove this shielding.

3. Remove the two screws from around the modulator. One is to the left of the RF jack, the other in front of the A/V jacks.

4. Remove the six screws which attach the cartridge tray to the PCB, case and black plastic connector. Note that the "middle" pair are different to the others - they are longer, and a silver colour.

5. Now gently lift the PCB (and cartridge tray and lower shielding) up out of the case. Remove the leads from the controller ports and power/reset switch PCB, and remove the lower metal shielding.

6. Slide the cartridge tray forwards, lifting it away from the PCB and connector. You can leave the connector attached to the PCB.

7. Turn over the PCB, with the component side up and the black cartridge connector towards you.

8. Note the PCB revision. It's printed in white ink near the centre of the PCB. For example: "NES-CPU-11". There is a white sticker on the PCB which tells you which type of console you have. For example, my U.K. model says "PAL-MTL" (MTL is short for Mattel). An American console says "NTSC", and a Hong Kong console says "PAL-ASI" (ASI probably short for Asia). Let me know if yours is different!

9. Find the lockout chip. "U10 CIC" will be printed above it on the PCB. (The U number is not relevant; "CIC" is.) The lockout chip on my console has the following text printed on it:

   3197A
© 1986 Nintendo
   9213 A

   This is for a U.K. model console. Other known numbers are 3193A (American), 3195A (European), and 3196A (Hong Kong). The chip has 16 pins.

10. Locate pin 4 of the lockout chip. This is on the row nearest to you, the fourth from the left.

11. You need to cut this pin, and bend it up and away from the PCB. You may need to bend a couple of capacitors on the PCB away from the lockout chip in order to get to it. If something goes wrong and the entire pin breaks off, don't worry - see the "How the Modification Works" section. It may help to desolder the pin first; you can use some desoldering braid for

this. Try and cut as close as possible to the PCB, so that a decent length is left attached to the chip.

A neater way of doing this would be so desolder the entire chip, bend out pin 4, and resolder the chip, leaving pin 4 sticking out. However, this is quite difficult if you don't have a special IC desoldering tool.

12. This step is optional. Things seem to work fine with pin 4 left unconnected. But you can connect it to ground if you like.

    Solder the length of wire from pin 4 to ground. Suitable places to connect to are pins 11, 12, 13, 14 or 15 of the lockout chip, since these are all grounded. Pin 15 is on the row furthest away from you, second from left.

13. That's it! You may want to test your NES before fitting it back together. Put the PCB back in the case and connect the power and controller connectors. Slide the cartridge tray into position, making sure the lip is below the PCB. Put a game cartridge in and switch on. Hopefully everything will work! To check whether the lockout chip has really been bypassed, switch on with no cartridge inserted. There should just be a blank screen, with no 'flashing' effect.

14. Now reassemble your console. Enjoy your new 'universal' NES!
