Preserving arcade games

Ange Albertini

Welcome to my talk!

So, I present this because:

- Gaming is COOL !!!
- Retro-gaming is TRENDY !!!

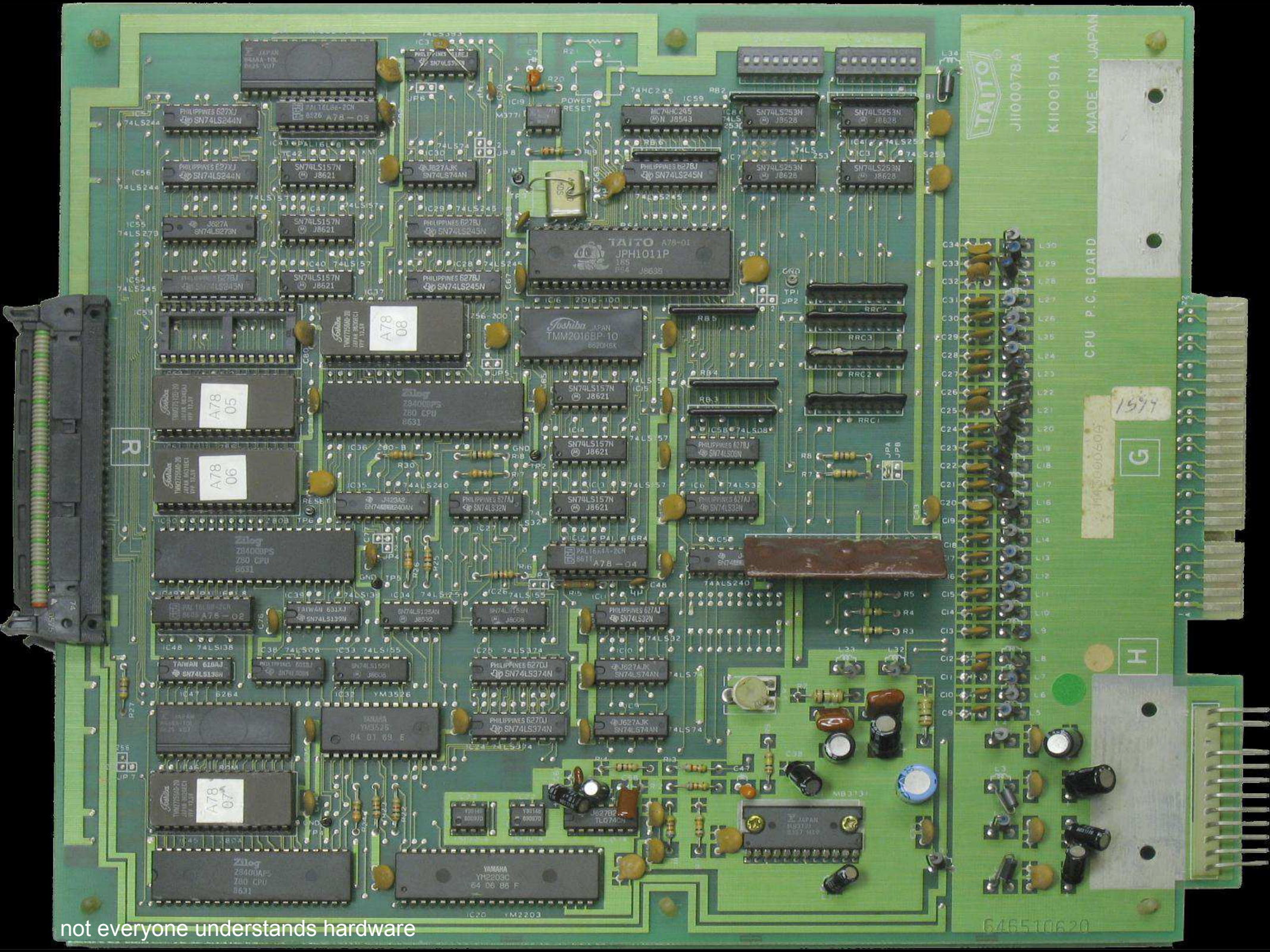
And more importantly,

- Arcade games are FUN !!!

So I made a ***really*** funny picture...


wow
so cool
much trendy
retro !!1!
very fun

...but I don't think that bullet point & memes
is the best way to talk about arcade games


TAITO
J1100078A
K1100191A
MADE IN JAPAN
CPU P.C. BOARD
JPH1011P
TMM2016BP-10
Z84008PS
Z80 CPU
YM2203C
YM3526
TL074CN
SN74LS374N
SN74LS245N
SN74LS157N
SN74LS253N
SN74LS244N
SN74LS32N
SN74LS240N
SN74LS139N
A78-01
A78-02
A78-03
A78-04
A78-05
A78-06
A78-07
A78-08
R
G
H
not everyone understands hardware

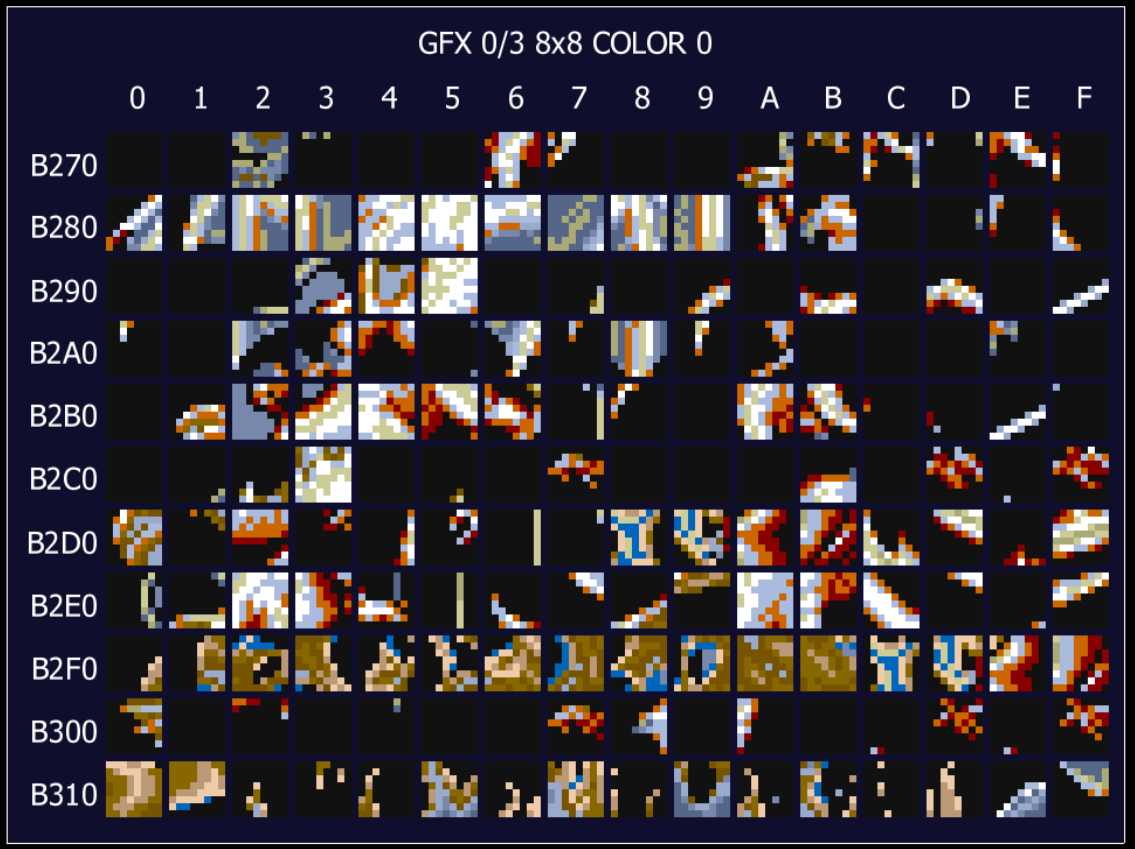
```
static MACHINE_CONFIG_START( tokio, bublbobl_state )

    /* basic machine hardware */
    MCFG_CPU_ADD("maincpu", Z80, MAIN_XTAL/4)   // 6 MHz
    MCFG_CPU_PROGRAM_MAP(tokio_map)
    MCFG_CPU_VBLANK_INT_DRIVER("screen", bublbobl_state,  irq0_line_hold)

    MCFG_CPU_ADD("slave", Z80, MAIN_XTAL/4) // 6 MHz
    MCFG_CPU_PROGRAM_MAP(tokio_slave_map)
    MCFG_CPU_VBLANK_INT_DRIVER("screen", bublbobl_state,  irq0_line_hold)

    MCFG_CPU_ADD("audiocpu", Z80, MAIN_XTAL/8)  // 3 MHz
    MCFG_CPU_PROGRAM_MAP(tokio_sound_map)

    MCFG_QUANTUM_TIME(attotime::from_hz(6000))

    MCFG_MACHINE_START_OVERRIDE(bublbobl_state,tokio)
    MCFG_MACHINE_RESET_OVERRIDE(bublbobl_state,tokio)

    /* video hardware */
    MCFG_SCREEN_ADD("screen", RASTER)
    MCFG_SCREEN_RAW_PARAMS(MAIN_XTAL/4, 384, 0, 256, 264, 16, 240)
    MCFG_SCREEN_UPDATE_DRIVER(bublbobl_state, screen_update_bublbobl)

    MCFG_GFXDECODE(bublbobl)
    MCFG_PALETTE_LENGTH(256)

    /* sound hardware */
    MCFG_SPEAKER_STANDARD_MONO("mono")

    MCFG_SOUND_ADD("ymsnd", YM2203, MAIN_XTAL/8)
    MCFG_SOUND_CONFIG(ym2203_config)
    MCFG_SOUND_ROUTE(0, "mono", 0.08)
    MCFG_SOUND_ROUTE(1, "mono", 0.08)
    MCFG_SOUND_ROUTE(2, "mono", 0.08)
    MCFG_SOUND_ROUTE(3, "mono", 1.0)
MACHINE_CONFIG_END
```

not everyone understands software


1UP
34760
HIGH SCORE
34760
INSERT
COIN
3
but everyone understand that it's a game!


HACKING
EMULATION
GAMES
that's the cool part of emulation:
it brings games to everyone !
(games that might be lost forever)

This talk is about arcade games,
the games where you put money to play.
That money would go in the operator's pocket,
no share to the arcade manufacturer.
To be successfull, they had to be awesome.
"Dedicated" (hardware, controls...) is the key to their success.



some arcade hardware graphics were cut into tiles:
the CPU can't draw directly: it just gives a list
of tile, then a dedicated chip draws the complete screen.
Smoother animation, but can't draw anything else.

NAOMI

Chihiro

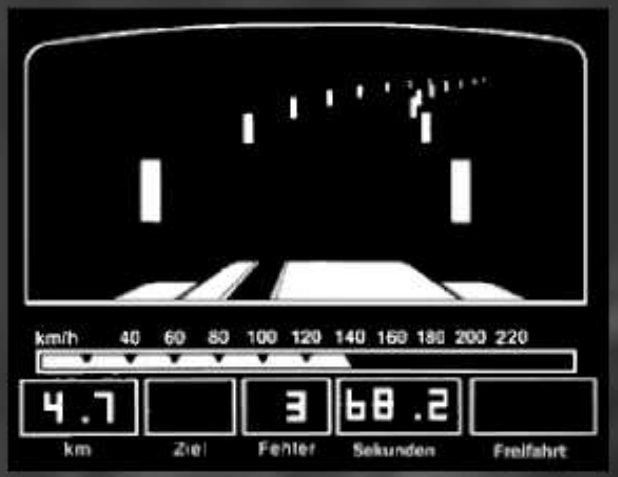
TRIFORCE

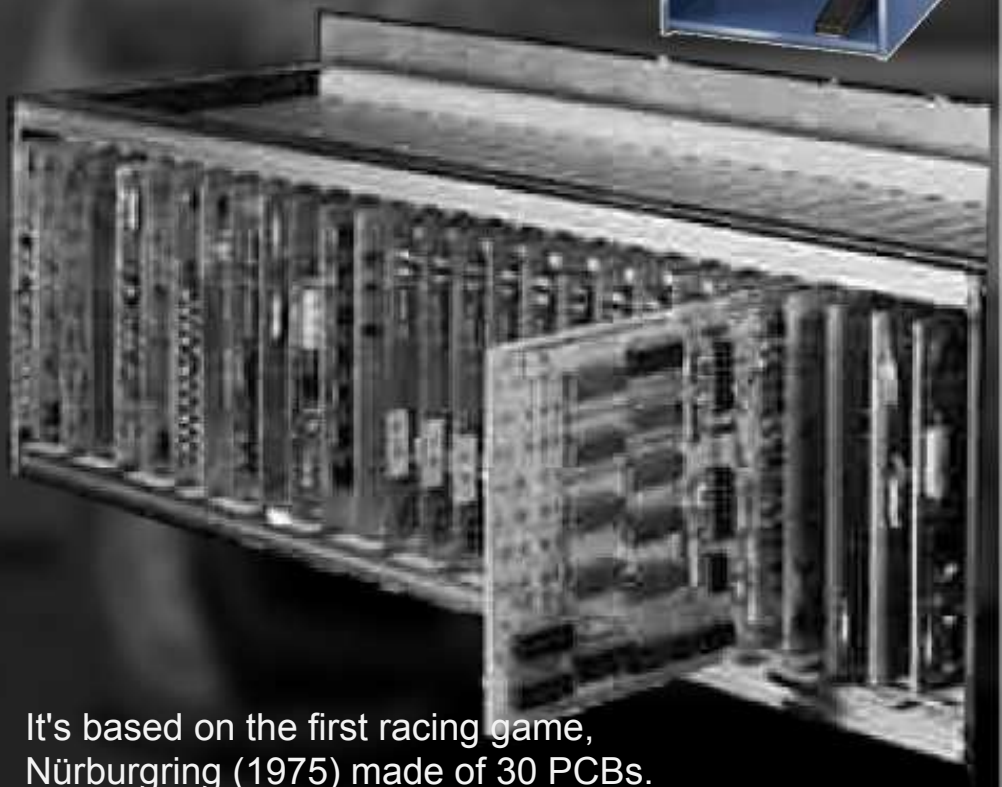
NAMCO · SEGA · NINTENDO

some arcade hardware were powered-up consoles,
but there were many more arcade hardwares.

Let's go back in time:
This is Night Driver (Atari 1976)...

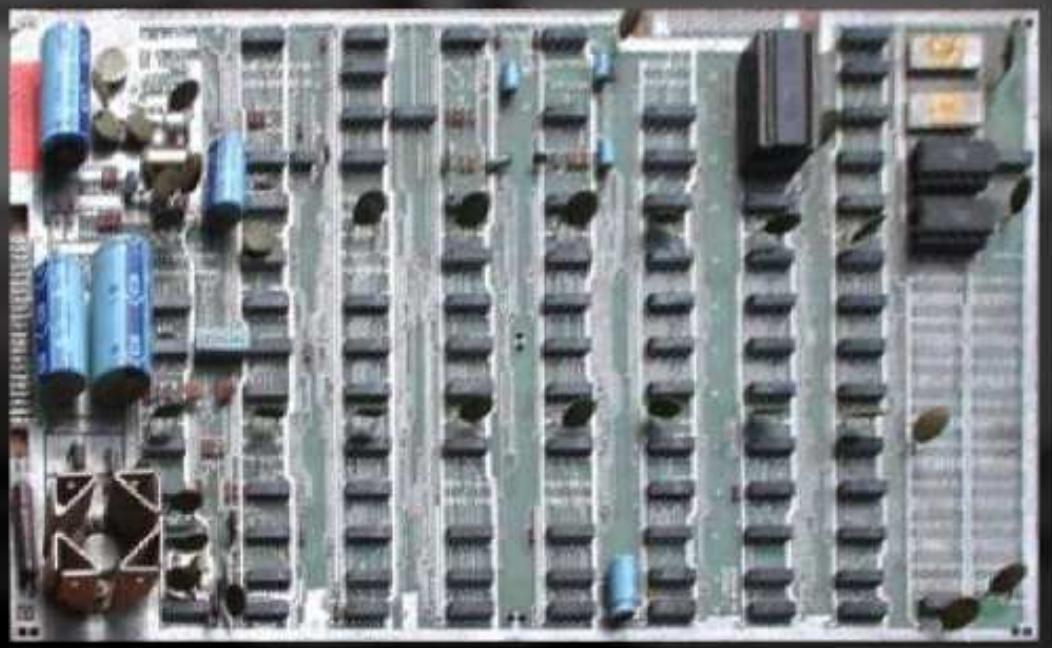
Nürburgring





It's based on the first racing game,
Nürburgring (1975) made of 30 PCBs.

NIGHT DRIVER




Berzerk was one of the first game with digitized speech.
It cost 1000 USD / word to be digitized
(it contained 16 words!)...
1. Object of game is to shoot as many Robots as possible and escape from room.
2. Player is controlled by control stick and can move in eight directions.
3. Aim with control stick and shoot with either FIRE button.
NOTE: Player stops moving when shot is fired.
4. Robots are worth 50 points. Bonus Score for destroying all Robots (even if Robots destroy each other).
6. EVIL OTTO comes out from position player started, cannot be destroyed, will go thru walls, and follows player with its object to destroy the player.
Extra man for score of 5,000.
DESIGNED AND PROGRAMMED BY:
15C-4

STERN GEHT BERZERK!

...they also made a german version !
same price per word ? ;)

STERN GEHT BERZERK!

Wenn Sie glauben, dass wir bei der Entwicklung von Berzerk aus dem Häuschen geraten sind, dann haben Sie recht! Wir haben hier erstmals unsere gesamte Technologie und all unser Wissen in ein einzelnes Video-Spiel gesteckt. Das Ergebnis ist ein Video-Meisterwerk, das nicht nur die Spieler absolut ausser Rand und Band geraten lässt, sondern das auch die Gewinne direkt zu den Operatoren treibt.

AUFZÄHLUNG INNOVATIVER BESONDERHEITEN VON BERZERK

- Unübertroffener Wortschatz von 30 Wörten lässt das Spiel zum Spieler Nachrichtenverkehr unterhalten.
- 64.000 beliebig angeordnete Modellvorlagen erscheinen in labyrinthischer Gestaltung für explosive, sich nicht wiederholende Action auf der Video-Platte.
- Ein vor kurzem entworfener Daumenhebel ermöglicht es dem Spieler, das Bild des Humanoiden in 8 verschiedene Richtungen zu bewegen.
- Nach Spielende erscheinen die bis dato erzielten 10 höchsten Punktgewinne auf dem Bildschirm.
- Selbst bei ausgeschaltetem Gerät speichert die Informationsdatei die bis dato erzielten 5 höchsten Punktgewinne.
- Betriebsart 'Anziehung' lockt Spieler mit der zeitlich programmierten Durchsage an: "Münzen in der Tasche entdeckt."
- Alle logischen Tafeln sind in leicht zugänglichem Ausziehfach im Vordergehäuse untergebracht, was mühelose Wartung gewährleistet.
- Hochentwickeltes automatisches Diagnoseprogramm.

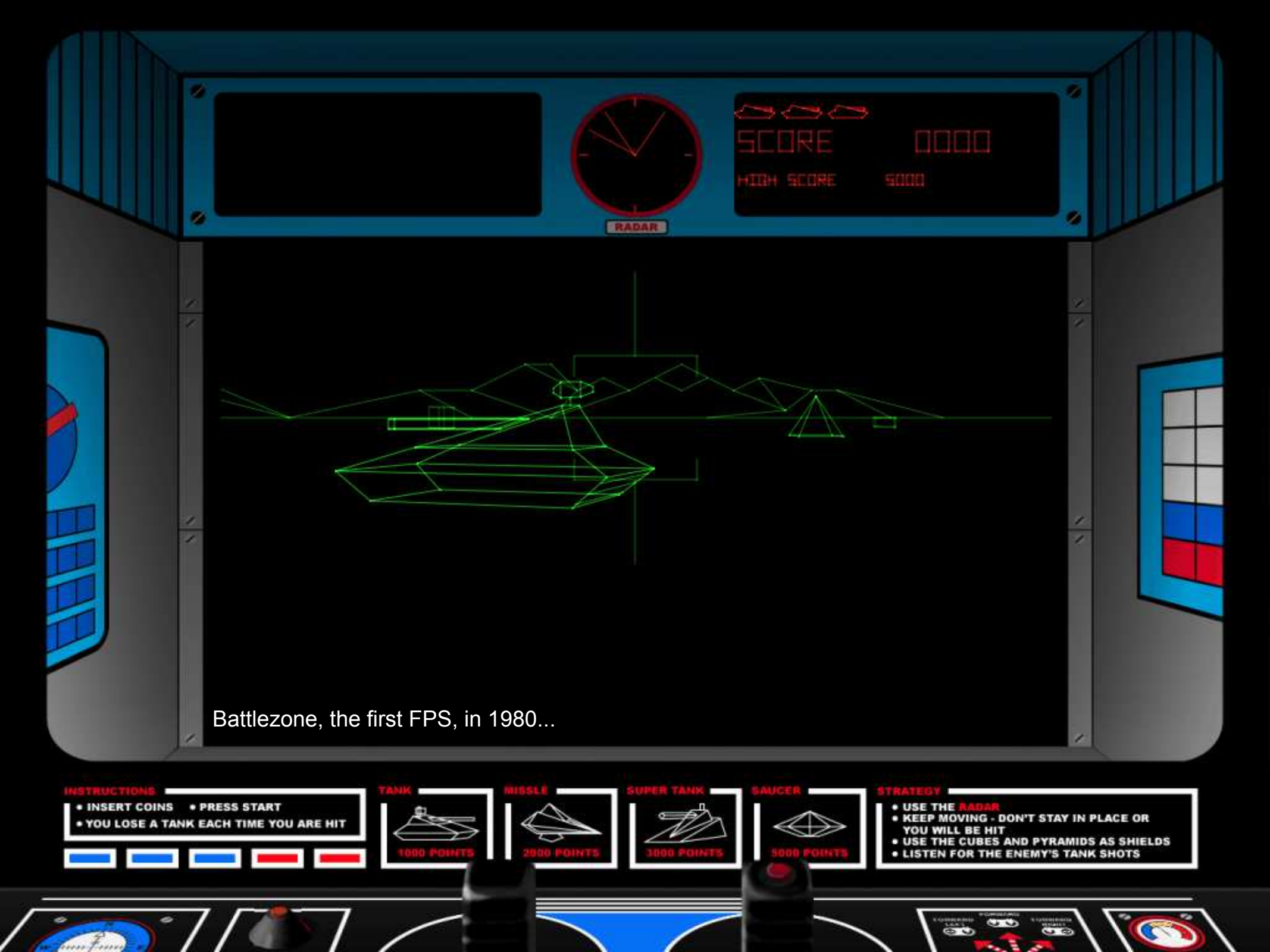
SPIELEIGENSCHAFTEN

Roboter verfolgen Humanoiden (Spieler) durch eine der 64.000 möglichen Modellvorlagen.

Humanoide vermeidet Roboter durch gekonnte Betätigung des Daumenhebels, und er vernichtet sie durch Feuerung seiner Geschosse.

Der "böse Otto," eine unzerstörbare Macht, erscheint aufs Geratewohl am Bildschirm, um den Humanoiden zu verfolgen und zu vernichten. Er muss um jeden Preis vermieden werden!

„Dieses Spiel haut wirklich jeden vom Stuhl! Auch Sie!"



Battlezone, the first FPS, in 1980...

...was initially designed as a military trainer.

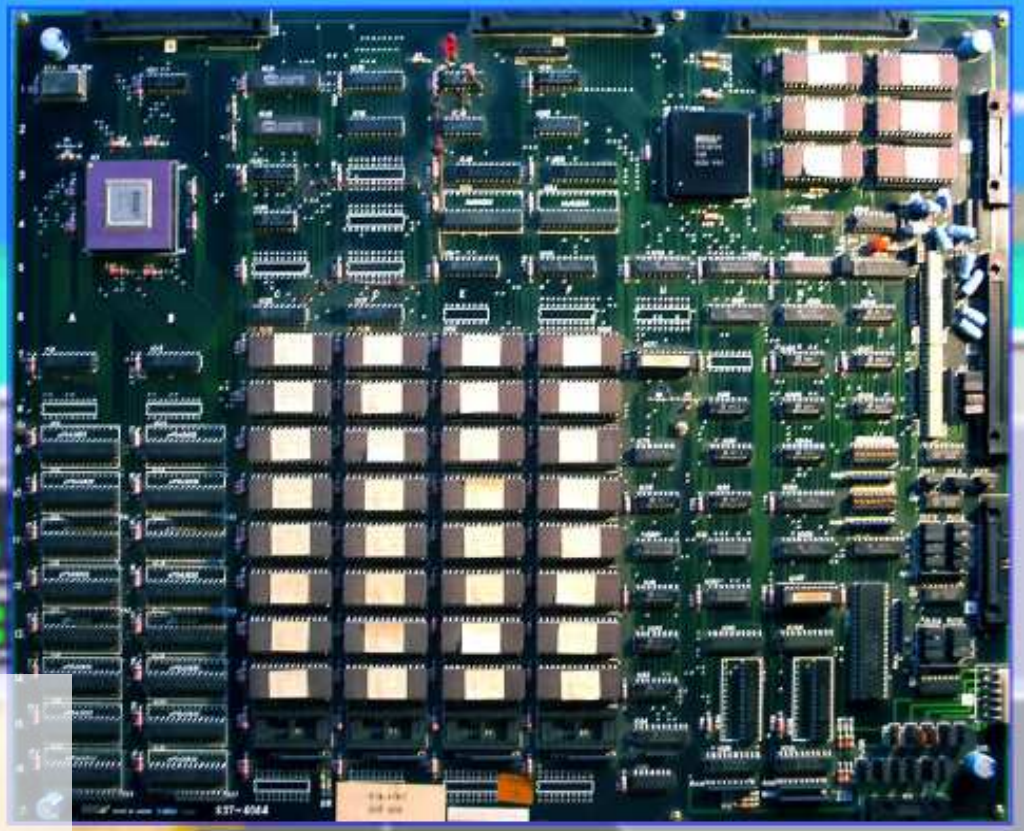
I, Robot (1984) a 3d action game with filled polygons

... is considered to be 'too advanced for its time'.

Dragon's Lair, an ‘interactive’ cartoon in 1983,
at a time where HDs were 10 Mb and graphics in 16 colors.

...was using the very recent Laser Disc technology (from 1981).
But LD drives were quickly worn out, because of frequent scene skipping.

Outrun (Sega 1986), awesome racing game!



...uses 2 main CPUs at 10 Mhz (an Amiga 500 runs at 7 Mhz)
the 2nd CPU's only task is to display the roads.
(they're drawn at 30 FPS *only*, the rest of the game at 60)

Hard Drivin (1989), a 3d simulation way before modern GPUs existed...

...used 3 PCBs.
They made a triple screen version of the sequel:
6 PCBs, 4 CPUs, 9 DSPs !!!!
It's emulated since last month (November 14) !

Sometimes, it was the arcade cabinet that was awesome.
Hang gliding, bike, car... ass poking ?!?

R360

Sega's R360 rotates the player on all axis, even upside down !

Sometimes, the screen was the awesome part: half sphere, 3x screen...


...and with awesome games came awesome piracy!

the first bootleg in Mame is from 1977!

As long as a game was good enough and its hardware not too extreme, bootlegs would be made. A few of them were 'creative'.


DARTH VADER
CRAZY KONG
VENUS
XEVIOS
BATTLES
NEXT PASE
Vautour
Condor
Griffon
FENIX
FX
ATOM
GRAN PREMIO F1
MONZA
KNIGHTBOY
Super BOBBLE BOBBLE
Mr. Dig
WEST STORY
TUMBLE POP
STONE AGE
ようへい LANSQUENET
Final CRASH
BEST LEAGUE
RAPID HERO
10th ANNIVERSARY ALL TEAM BATTLE
THE KING OF FIGHTERS EXTRA PLUS
SNK PLAYMORE
INSERT COIN
SNK PLAYMORE ©SNK PLAYMORE 2005 WINTER
臥虎藏龍
CROUCHING TIGER HIDDEN DRAGON
SUPER PLUS
METAL SLUG 6
Space Invaders (text) <> Darth Vader (gfx)
Metal Slug 3 <> Metal Slug 6 (!!)

They went further and were taking a good game,
then hacking gfx & sound to create a 'new' game

or sometimes they just ripped off graphics,
to make a (crappy) game,
like a shooter with StarCraft's GFX :(

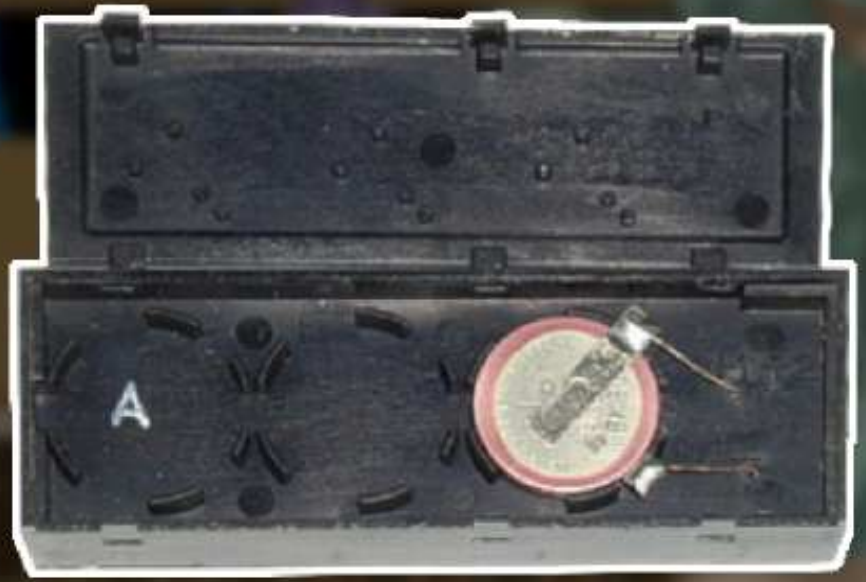
With awesome piracy came awesome protections.
once again, dedicated stuff, sometimes
tightly integrated with the game internals

In Bee Storm, if the protected CPU is missing,
the game works, but the enemies don't shoot anymore.

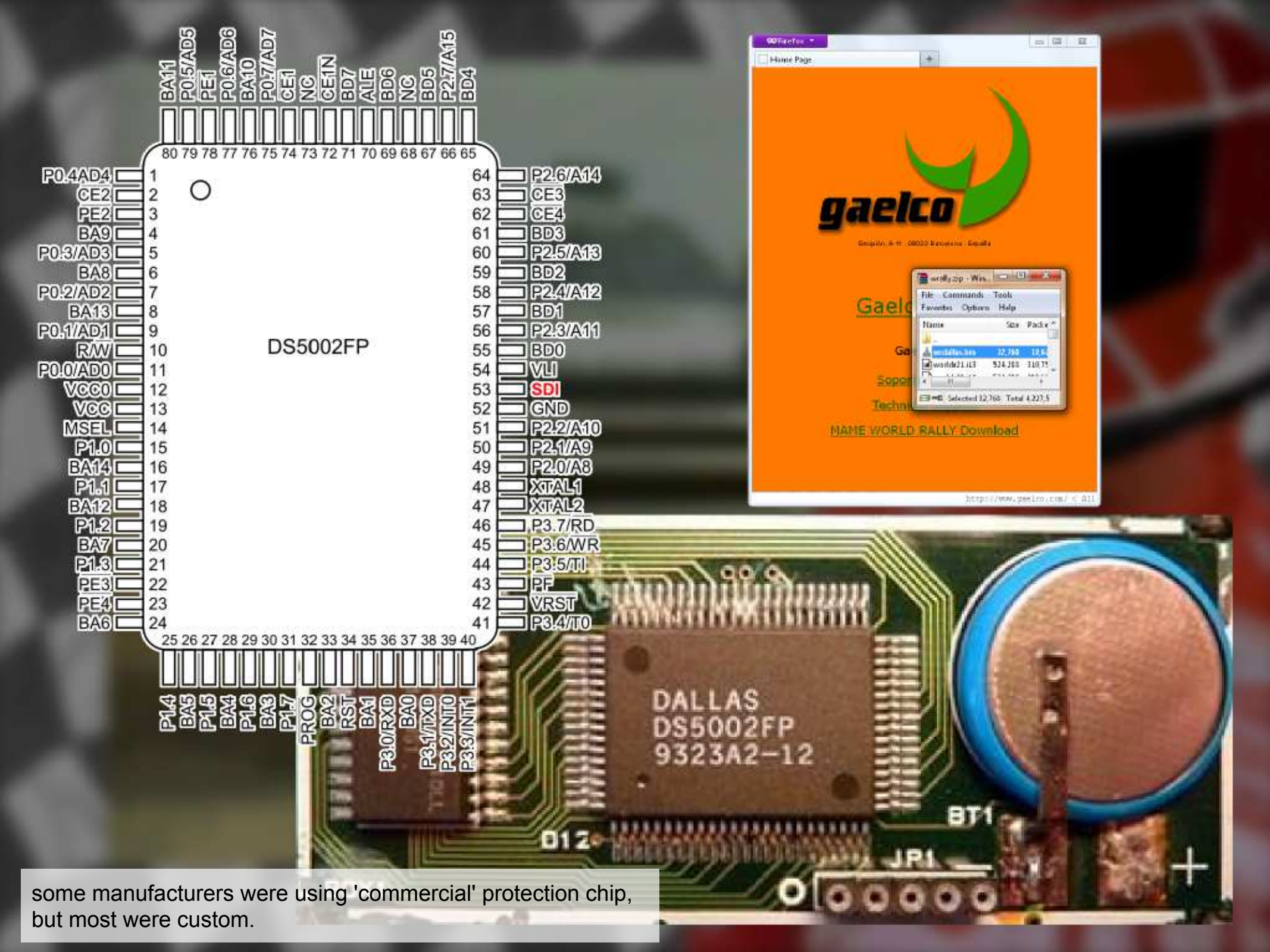
In Hang-on, if the 2nd CPU (sometimes encrypted) is missing, then roads are straight.

in S.P.Y., collisions are handled by a custom chip: without it, you can't hurt and cannot be hurt.

So, in general, the only solution to correctly emulate
them is to decap the protection chip and read the internal ROM.
Bubble Bobble was only correctly preserved in 2005 !

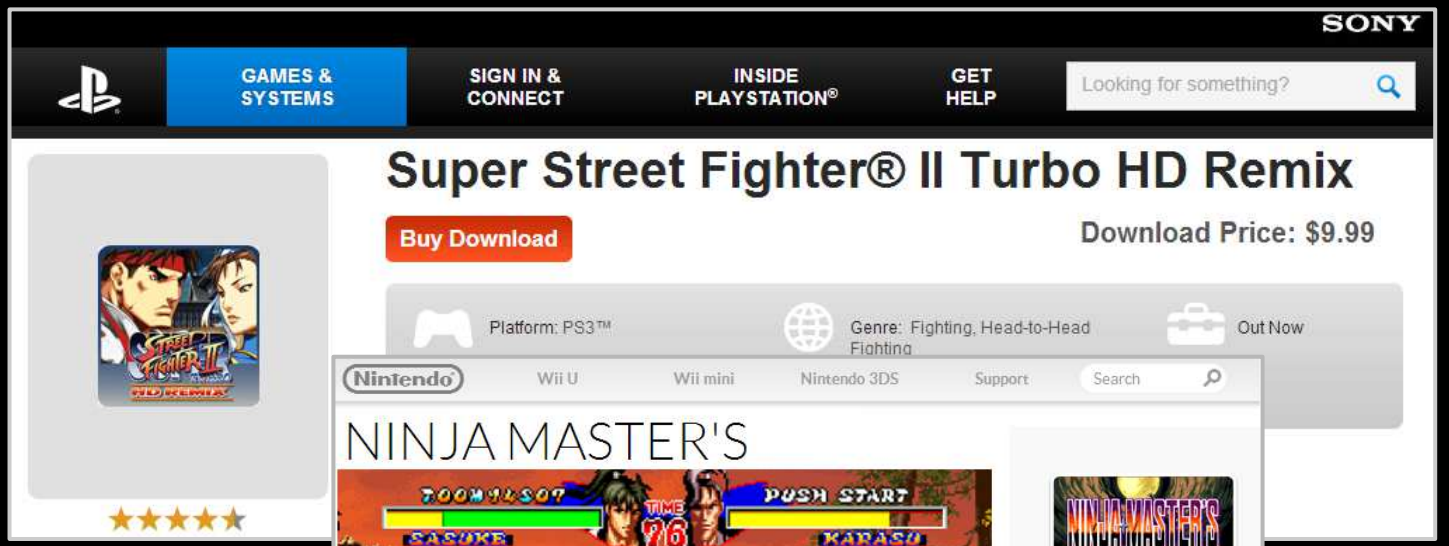


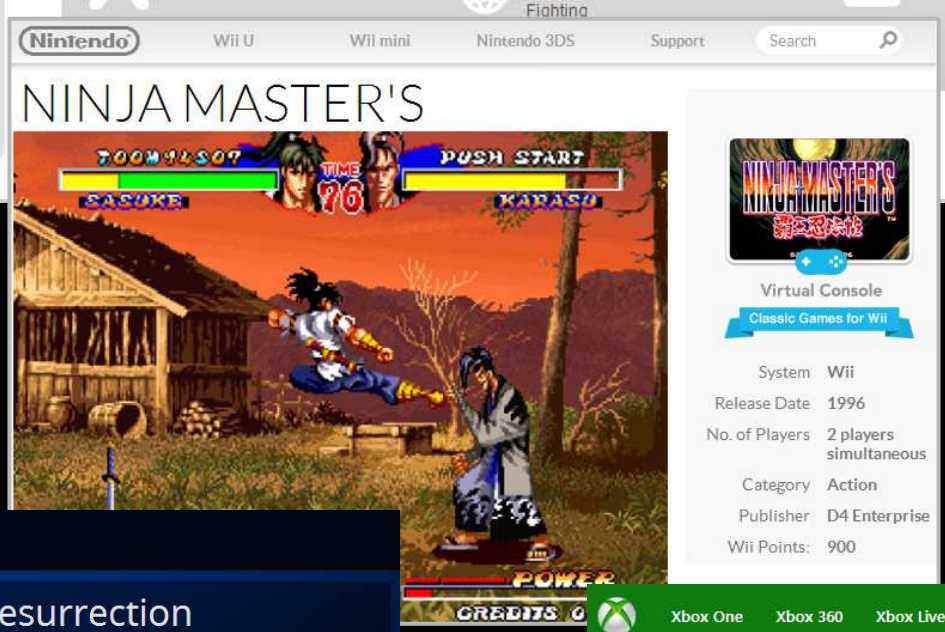
to store protected data, they went further:
store data on battery-powered RAM.
the battery dies, the game dies.
the manual doesn't even mention it!
the warranty is void if you open the game's case!

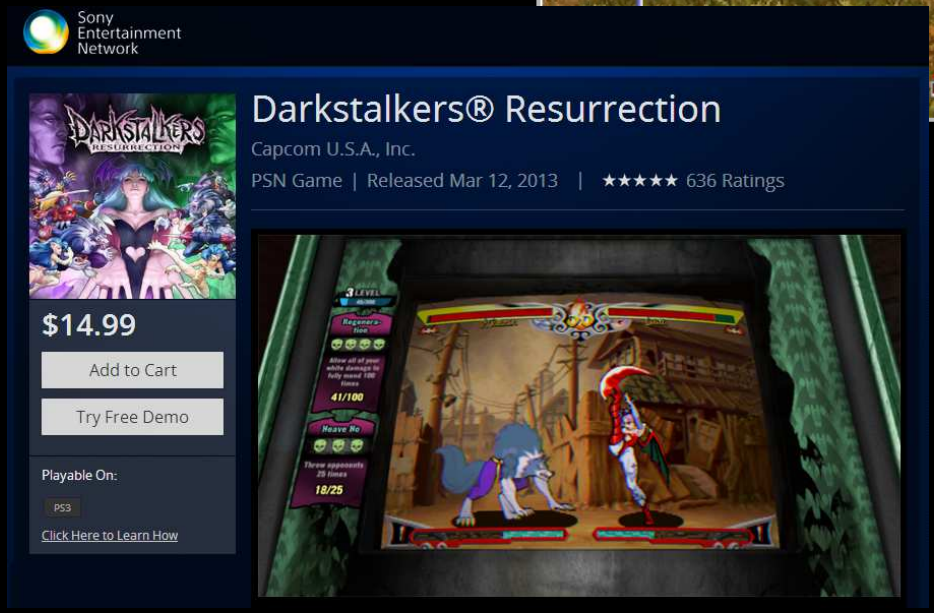


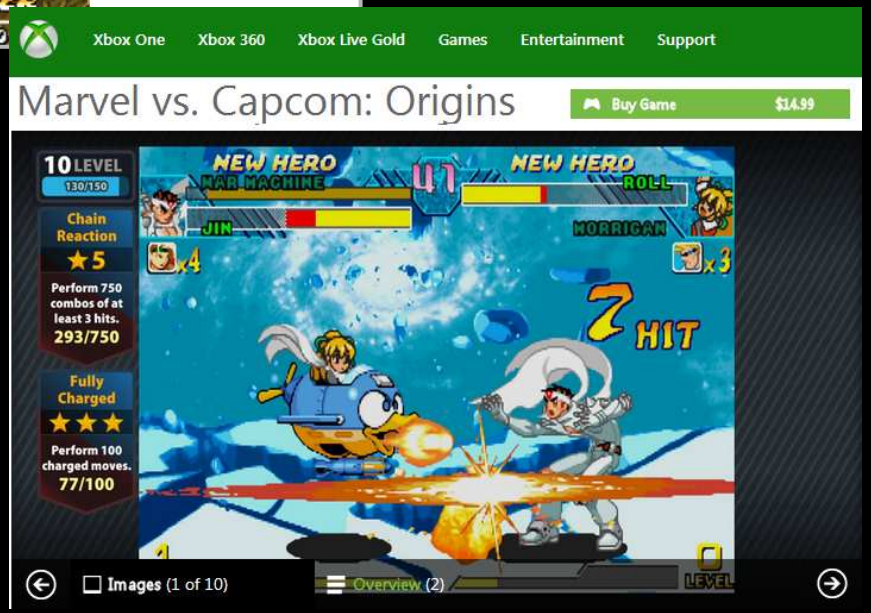
some manufacturers were using 'commercial' protection chip, but most were custom.

so you're not supposed to open the game,
yet all games will eventually die once all batteries are empty.
Hacking these games is the only way to preserve them.









it also enables the IP to be re-used commercially later.

Darkstalkers® Resurrection - B.B. Hood Arcade Cabinet

Capcom U.S.A., Inc.

Add-On | Released Mar 26, 2013 | ★★★★☆ 10 Ratings

$0.99

Add to Basket

Playable On:

PS3

Click Here to Learn How

TEEN Blood Partial Nudity

More for Darkstalkers® Resurrection

Explore more games and downloadable content for Darkstalkers® Resurrection!

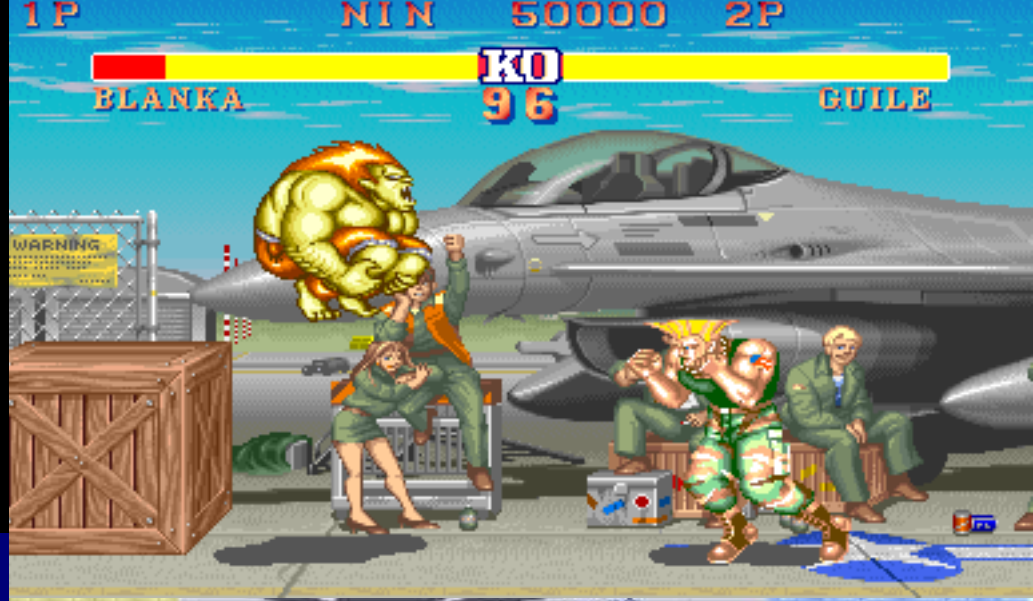
Description

Customize the look of your arcade cabinet view mode with this skin based on the evil Darkhunter, B.B. Hood.

modern practices also brought DLC rip-offs :(

Arcade games had to be awesome. They were often using dedicated parts.
they were heavily pirated. they were heavily protected.
So protected that it makes them vulnerable (to time)!
Hacking is the only way to preserve them.


CAPCOM
CP SYSTEM
SER No. 006000413
LOT No.
CAPCOM CO. LTD.
CAPCOM
Let's look at the Capcom Play System, known as CPS1.



known mostly for Street Fighter II

and many other good games

the complete list...

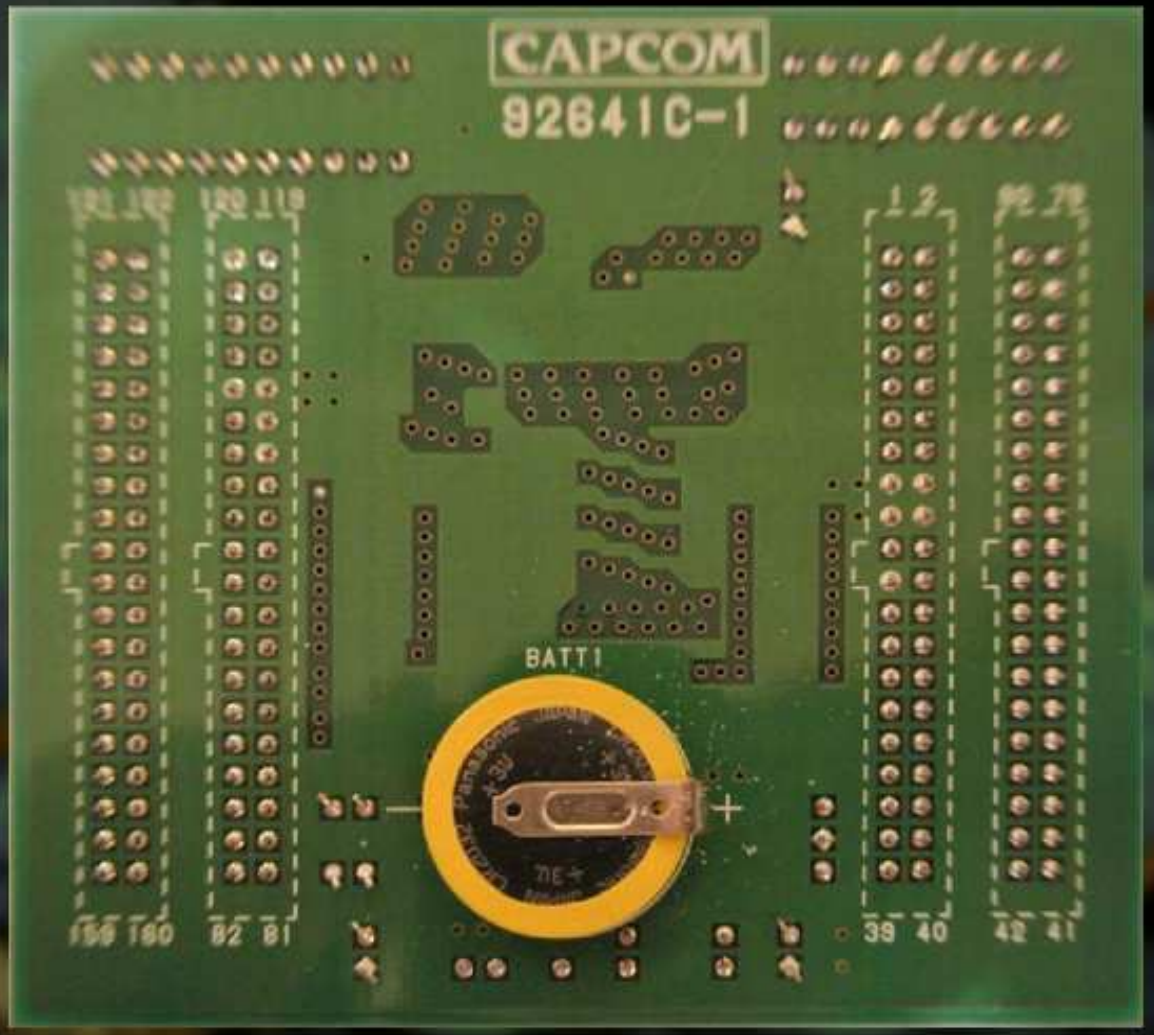
including the least known, only emulated in June 2014. It's SF2-based, but it's a mole hitting game !!

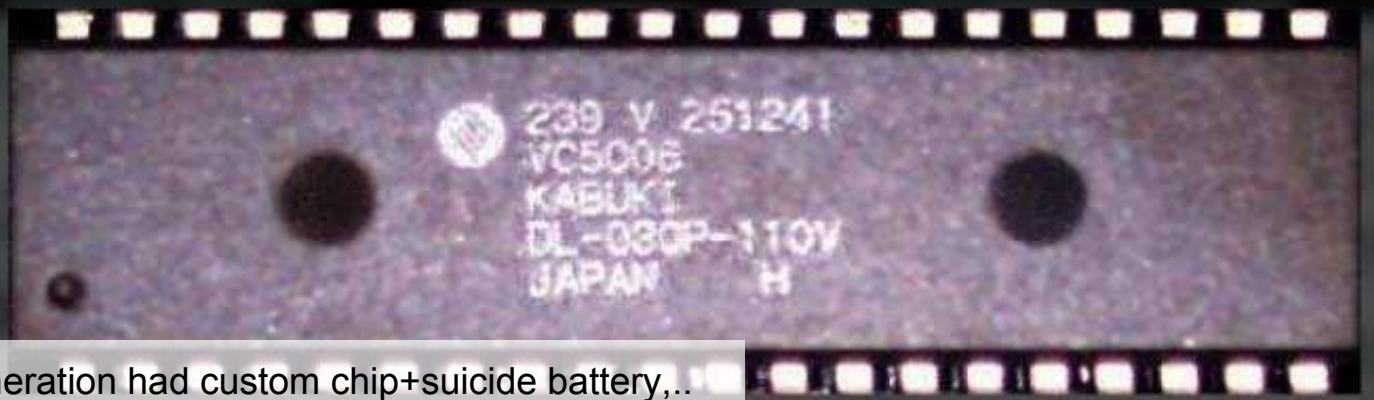
CPS1 was increasingly protected:
Yet it was completely hacked.
SF2 bootlegs were common.

a final fight bootleg, adding extra characters to control.

an original CPS1… (3 PCBs)

and a CPS1 bootleg (nothing in common)





the latest CPS1 generation had custom chip+suicide battery,..

...but it was defeated nonetheless:
weak encryption+encrypted data made plaintext attack easy.

CPS1 was great.
It was protected.
It was completely hacked.

Capcom released its evolution, the CPS2

it started with this...

from Super SF2 (1993)
to Hyper SF2 (2003)
(how original !)


GHTY COMBO
FINISH
K.O.
ATTACK
CPS2 was awesome...


INSERT 2 COINS
PUSH START BUTTON
SCORE
0001530
EASY
1P 69540
TOP 1000000
2P 0
POW
1P- 2000
2P- 6000
3P- 2100
P-Warrior
9700
WARRIOR
PRESS START
VULCAN 40/40
VULCAN 60/60
VULCAN 40/40
Red Dragon
...really awesome!

...plenty of great games...

I

II

III

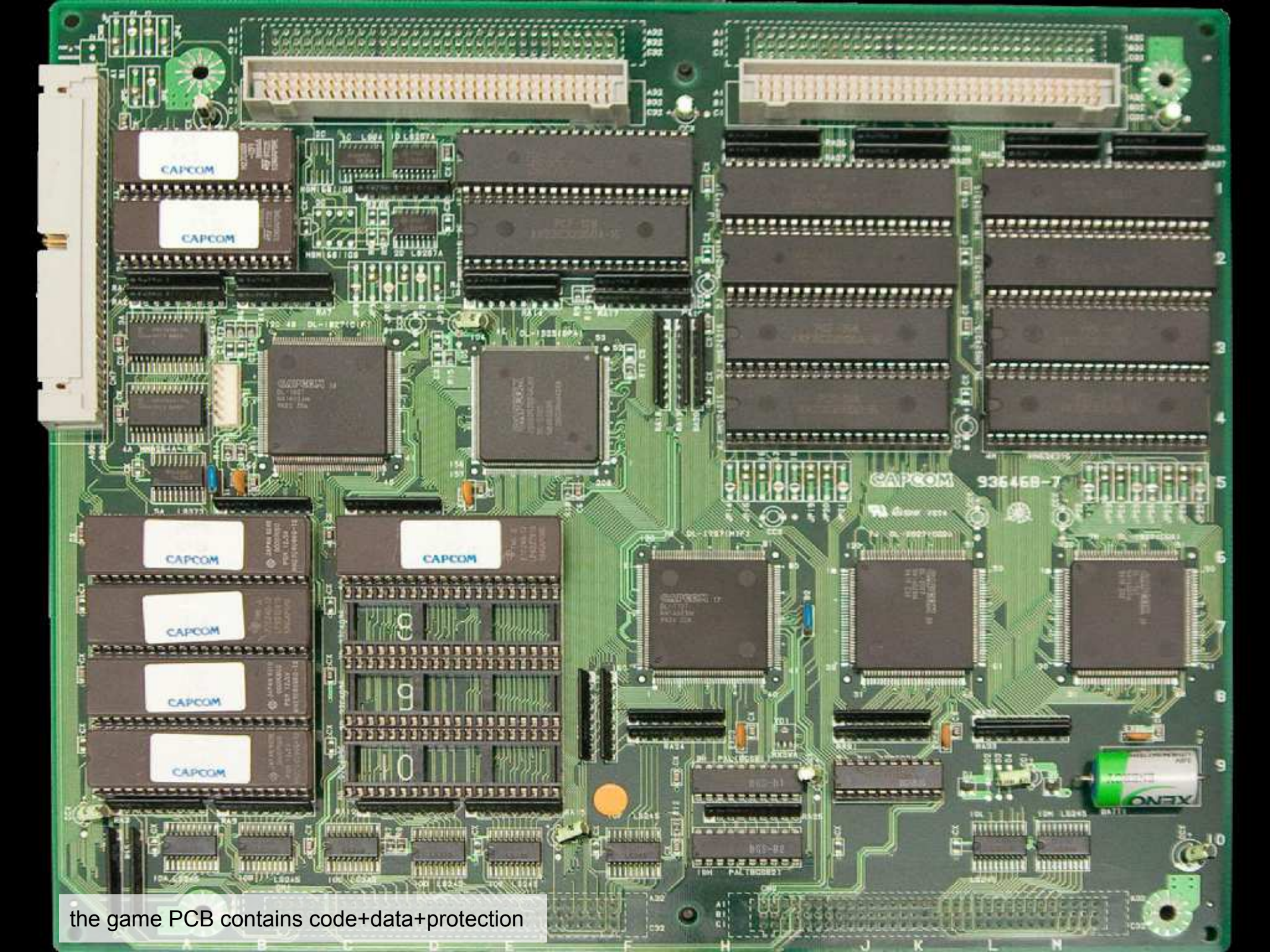
the real successor to the CPS1
the last successful hardware from Capcom.

here is the complete list of bootlegs, hacks, swaps...
(absolutely NOTHING)

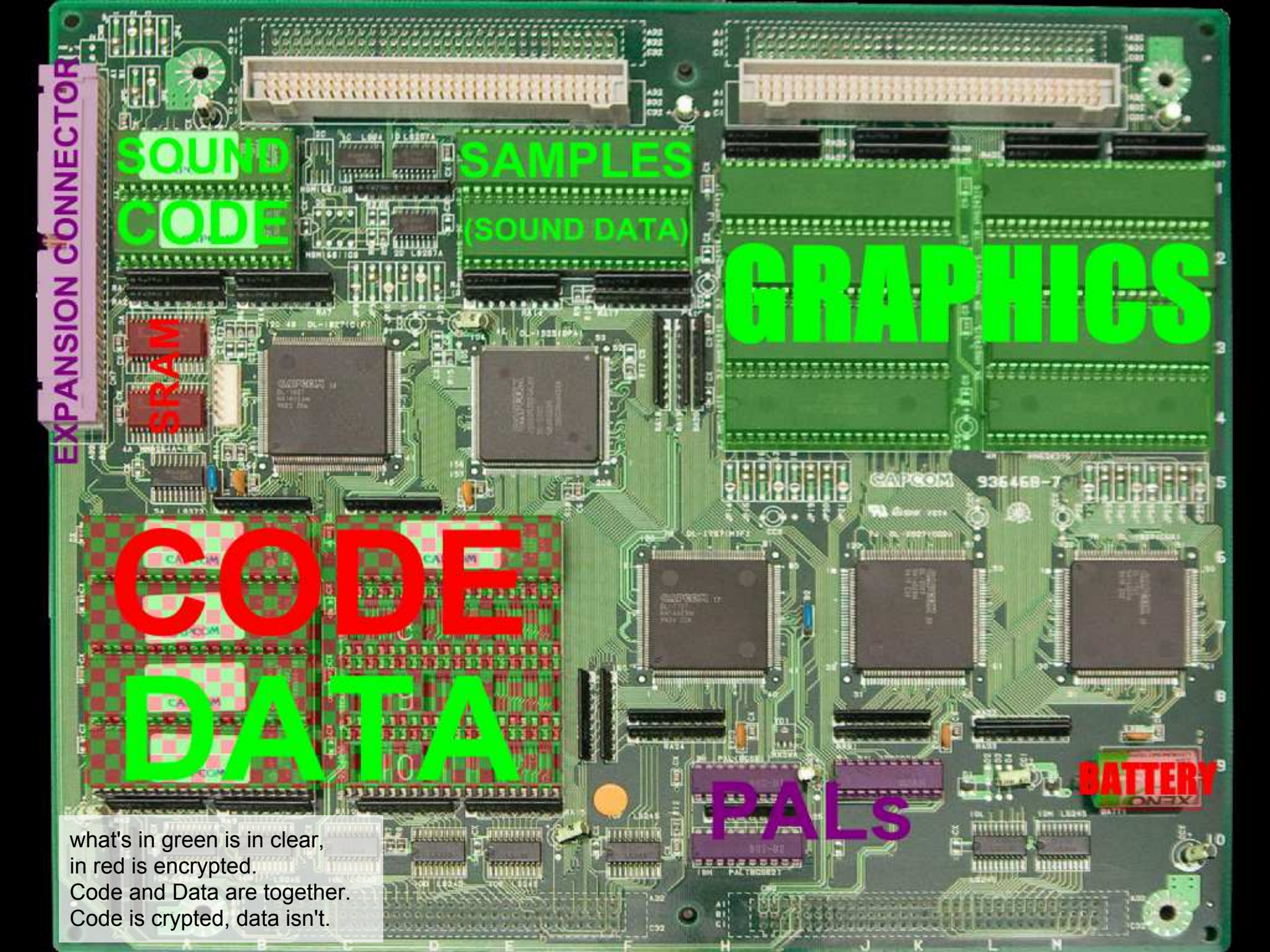
they were so desperate that they couldn't hack that...

that they hacked a console version into an arcade game (with typo)


CP II
SYSTEM
B-cartridge
CAPCOM
Main Board
Connectors
U.S.A.
A CPS2 is a sandwich of 2 PCBs
(sometimes only 1, sometimes 3)



the game PCB contains code+data+protection


EXPANSION CONNECTOR
SOUND CODE
SAMPLES (SOUND DATA)
GRAPHICS
SRAM
CODE DATA
PALs
BATTERY
what's in green is in clear,
in red is encrypted.
Code and Data are together.
Code is crypted, data isn't.

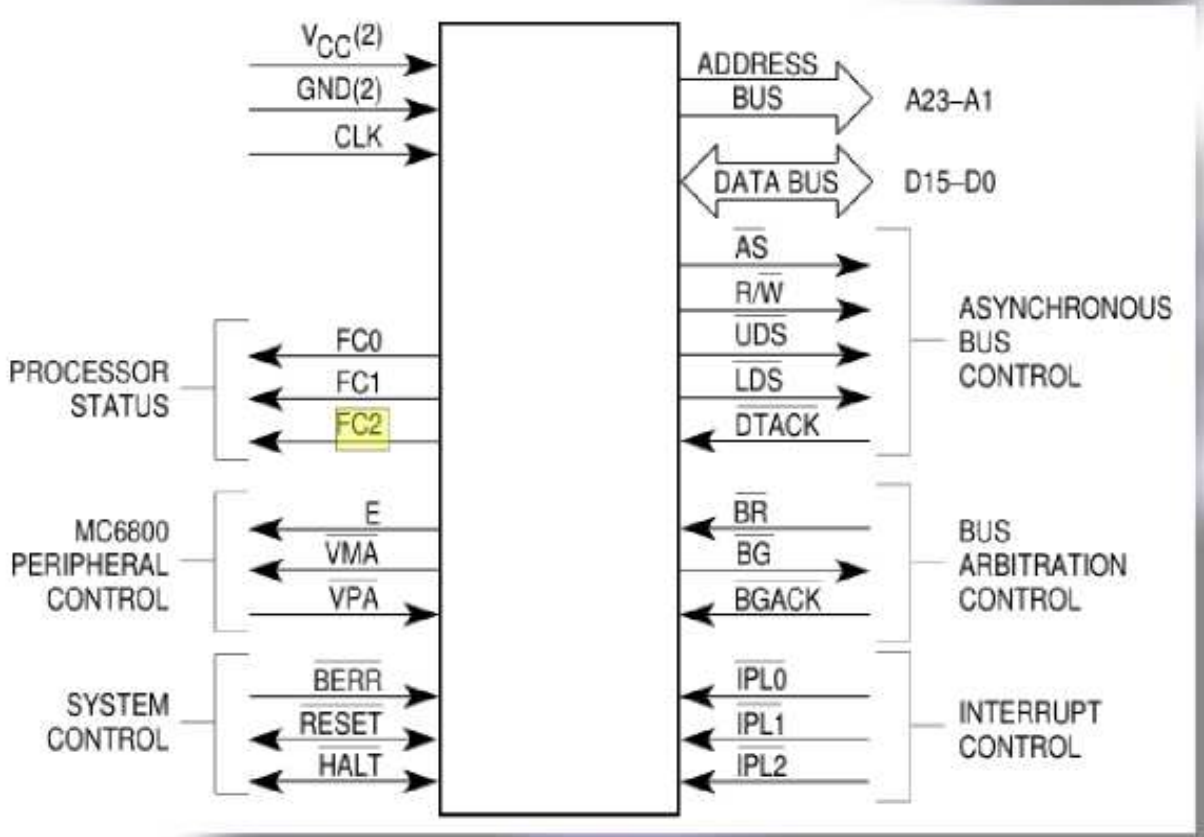


Table 3-3. Function Code Outputs

Function Code Output			Address Space Type
FC2	FC1	FC0	
Low	Low	Low	(Undefined, Reserved)
Low	Low	High	User Data
Low	High	Low	User Program
Low	High	High	(Undefined, Reserved)
High	Low	Low	(Undefined, Reserved)
High	Low	High	Supervisor Data
High	High	Low	Supervisor Program
High	High	High	CPU Space

Table 6-2. Exception Vector Assignment

Vectors Numbers		Address		Space[6]	Assignment
Hex	Decimal	Dec	Hex		
0	0	0	000	SP	Reset: Initial SSP[2]
1	1	4	004	SP	Reset: Initial PC[2]
2	2	8	008	SD	Bus Error
3	3	12	00C	SD	Address Error

assigned these numbers.

2. Reset vector (0) requires four words, unlike the other vectors which only require two words, and is located in the supervisor program space.

The spurious interrupt vector is taken when there is a bus error

decryption is made on the fly,
during memory fetch.
read standard memory? as is.
read for execution? decrypt.

patch an opcode (unknown encryption)
→ black screen. game over. retry ?

CPS2 was really awesome.
it was well protected.
it was absolutely unscathed for 6 years.

Capcom had a major competitor.

the Neo-Geo is known for many games...

an exceptional success and longevity !

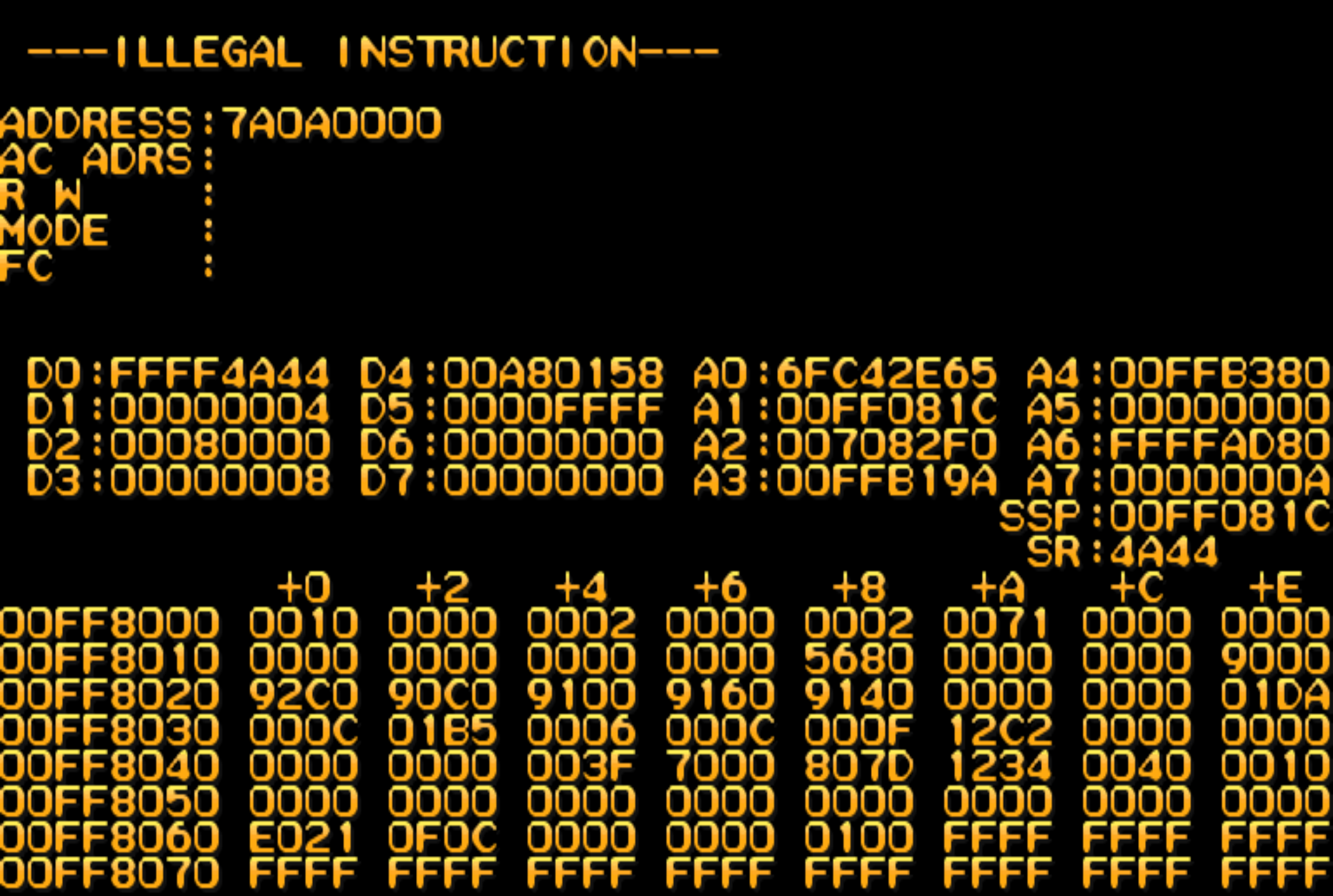
a success in arcade AND as an expensive console

Capcom created something
that made the NeoGeo look small and cheap.
It was a commercial failure...


STREET FIGHTER ZERO
950605
JAPAN
WORK RAM OK
CPS0 RAM OK
CPS1 RAM OK
CPS2 RAM OK
OBJECT RAM OK
Q SOUND RAM OK
VIRTUAL AUDIO
QSOUND
CAPCOM
STREET FIGHTER ZERO
INSERT COIN
©CAPCON Co., Ltd. 1995
PLAYER SELECT
INSERT COIN
79
STREET FIGHTER ZERO
951020
CPS CHANGER
WORK RAM OK
CPS0 RAM OK
CPS1 RAM OK
CPS2 RAM OK
STREET FIGHTER ZERO
PRESS START
©CAPCON Co., Ltd. 1995
PLAYER SELECT
PRESS START
77
RYU
as a last effort, they backported a recent CPS2 game.
the first decrypted CPS2 port !!!


but nothing happened. the dragon was still alive.

to defeat a dragon, you need adventurers:
Razoola, Charles MacDonald, Andreas Naive, Nicola Salmoria, David Haywood, and many others.
(I worked with Razoola, and helped him on the PC side)



In November 1999, Razoola re-enabled SFZ's internal debugger (first working CPS2 patch !)
→ not blind anymore !

in spring 2000, he found that some specific memory ranges were not using encryption!
why ? no reason - just a big facepalm !
→ shellcode execution for a split second.

Mode	Generation	Syntax
Register Direct Addressing		
Data Register Direct	EA=Dn	Dn
Address Register Direct	EA=An	An
Absolute Data Addressing		
Absolute Short	EA = (Next Word)	(xxx).W
Absolute Long	EA = (Next Two Words)	(xxx).L
Program Counter Relative Addressing		
Relative with Offset	EA = (PC)+d_{16}	(d_{16},PC)
Relative with Index and Offset	EA = (PC)+d_8	(d_8,PC,Xn)
Register Indirect Addressing		
Register Indirect	EA = (An)	(An)
Postincrement Register Indirect	EA = (An), An ← An+N	(An)+
Predecrement Register Indirect	An ← An–N, EA=(An)	-(An)
Register Indirect with Offset	EA = (An)+d_{16}	(d_{16},An)
Indexed Register Indirect with Offset	EA = (An)+(Xn)+d_8	(d_8,An,Xn)
Immediate Data Addressing		
Immediate	DATA = Next Word(s)	#<data>
Quick Immediate	Inherent Data	
	EA = SR, USP, SSP, PC, VBR, SFC, DFC	SR,USP,SSP,PC, VBR, SFC,DFC

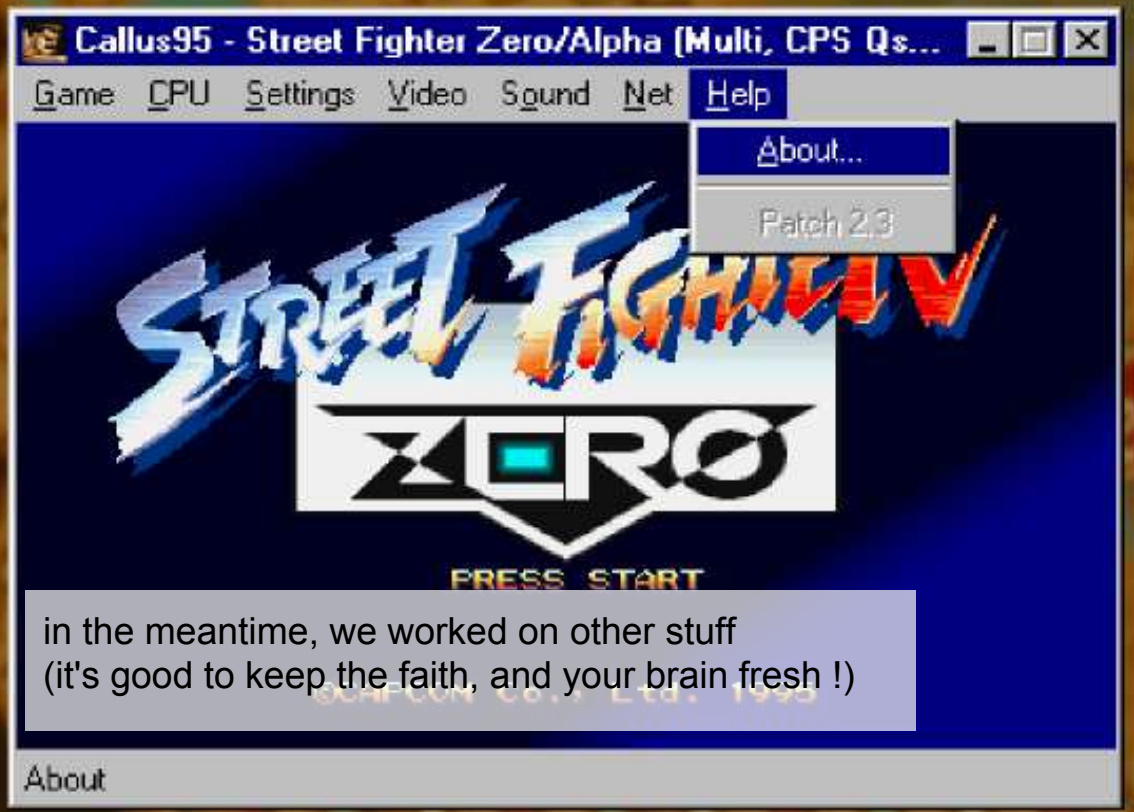
when reading relatively to code (PC), memory fetches are actually decrypted ! Sega prevented that, but Capcom failed.
→ first CPS2 decryption, word by word

This mode is similar to the mode described in **2.2.7 Address Register Indirect with Index (8-Bit Displacement) Mode**, except the PC is the base register. The operand is in memory. The operand's address is the sum of the address in the PC, the sign-extended displacement integer in the extension word's lower eight bits, and the sized, scaled, and sign-extended index operand. The value in the PC is the address of the extension word. This is a program reference allowed only for reads. The user must include the displacement, the PC, and the index register when specifying this addressing mode.

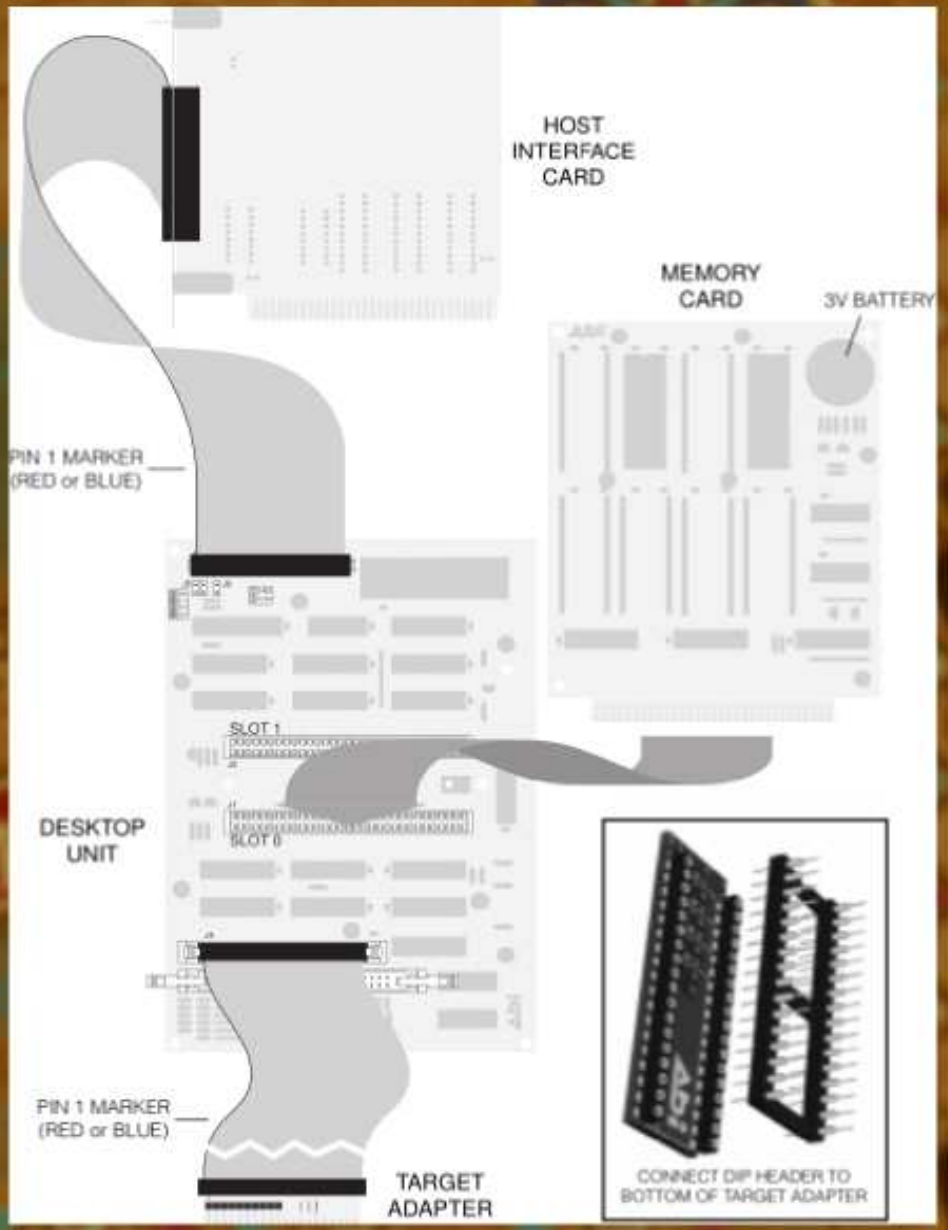
so, in Summer 2000, I visited Raz, hoping we'd break the algo.
but no success...

Zip File Password Cracking - Tutorial by Crashtest

"Well a long overdue essay on the vagaries of zip password cracking, how many times have you as a reverser been asked by someone "how do I crack a password protected zip?", I'll bet its a few :), well here is a little document by Crashtest explaining the main techniques". "Edited by CrackZ".



in the meantime, we worked on other stuff
(it's good to keep the faith, and your brain fresh !)



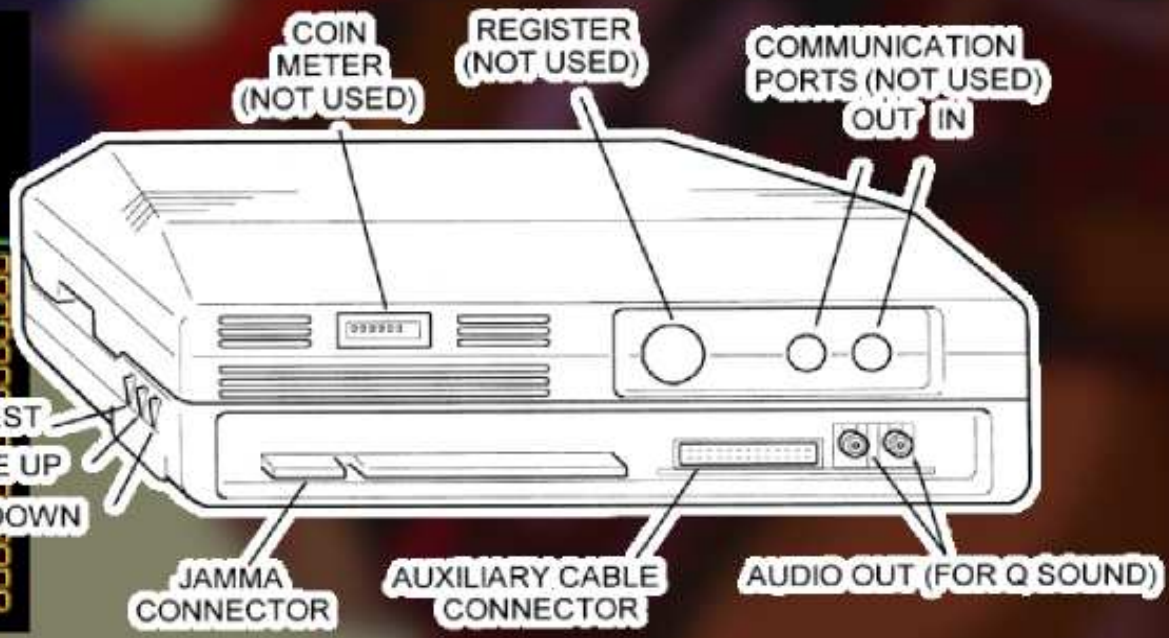
```
reset
nop
nop
nop
move.b   #$80, $800030.l
nop
nop
nop
nop
nop
nop
nop
nop
move.b   #$0, $800030.l
cmpi.l   #$5642194, D0
lea      ($6,PC), A4
bra      $d82
```

```
lea      ($6,PC), A2
bra      $ef6
jmp      (A4)
moveq    #$1f, D7
move.l   #$f000f000, D0
cmpi.l   #$5642194, D0
move.l   (A0)+, (A1)
or.l     D0, (A1)+
move.l   (A0)+, (A1)
or.l     D0, (A1)+
move.l   (A0)+, (A1)
or.l     D0, (A1)+
move.l   (A0)+, (A1)
or.l     D0, (A1)+
move.l   (A0)+, (A1)
or.l     D0, (A1)+
```

```
lea      ($6,PC), A2
bra      $d96
jmp      (A4)
moveq    #$1f, D7
move.l   #$f000f000, D0
move.l   (A0)+, (A1)
or.l     D0, (A1)+
move.l   (A0)+, (A1)
or.l     D0, (A1)+
move.l   (A0)+, (A1)
or.l     D0, (A1)+
move.l   (A0)+, (A1)
or.l     D0, (A1)+
move.l   (A0)+, (A1)
or.l     D0, (A1)+
move.l   (A0)+, (A1)
```

in December 2000, Raz noticed that Capcom leaked the key to keep decryption alive.
→ automated dump is now possible !

we dumped by connecting the CPS2 to the joystick port of the PC.
ugly, clumsy, slow, but worked !




Game CPU Settings Video Sound Net Help
STREET FIGHTER ZERO
950727
JAPAN
System reset
CS0


Game CPU Settings Video Sound Net Help
VIRTUAL AUDIO
QSOUND™
©Sound Chips have been developed by ©Sound and incorporate QSound's proprietary ©Sound sound enhancement technology.
CAPCOM
System reset
CS0


Game CPU Settings Video Sound Net Help
Jan 2001: first cps2 emulation
INSERT 2 COINS
CONTINUE REQUIRES ONLY 1 COIN
©CAPCOM Co., Ltd. 1995
System reset
CS0


Game CPU Settings Video Sound Net Help
TIME
RYU
KEN
System reset
CS0

Slashdot

stories
submissions
popular
blog
ask slashdot
book reviews
games
idle
yro

CPS-2 Encryption Scheme Broken

Posted by **Hemos** on Sunday January 07, 2001 @10:44AM
from the more-roms-for-all dept.

Acheon writes:

> "The CPS-2 arcade board from Capcom uses some hard encryption scheme that has been a very hot issue in emulation for years. Yet finally the code was broken Final Burn, a quite recent arcade emulator, showed concrete results by running previously unsupported games such as Street Fighter Zero using decrypted ROM images. The CPS-2 Shock Team, who managed to reverse engineer the process for scratch, really outdone themselves and it is a very uncommon achievement."

the news didn't get it right, as usual...

The Register®

CPS2 arcade encryption smashed

Morality debate ensues

By **Lucy Sherriff** • **Get more from this author**

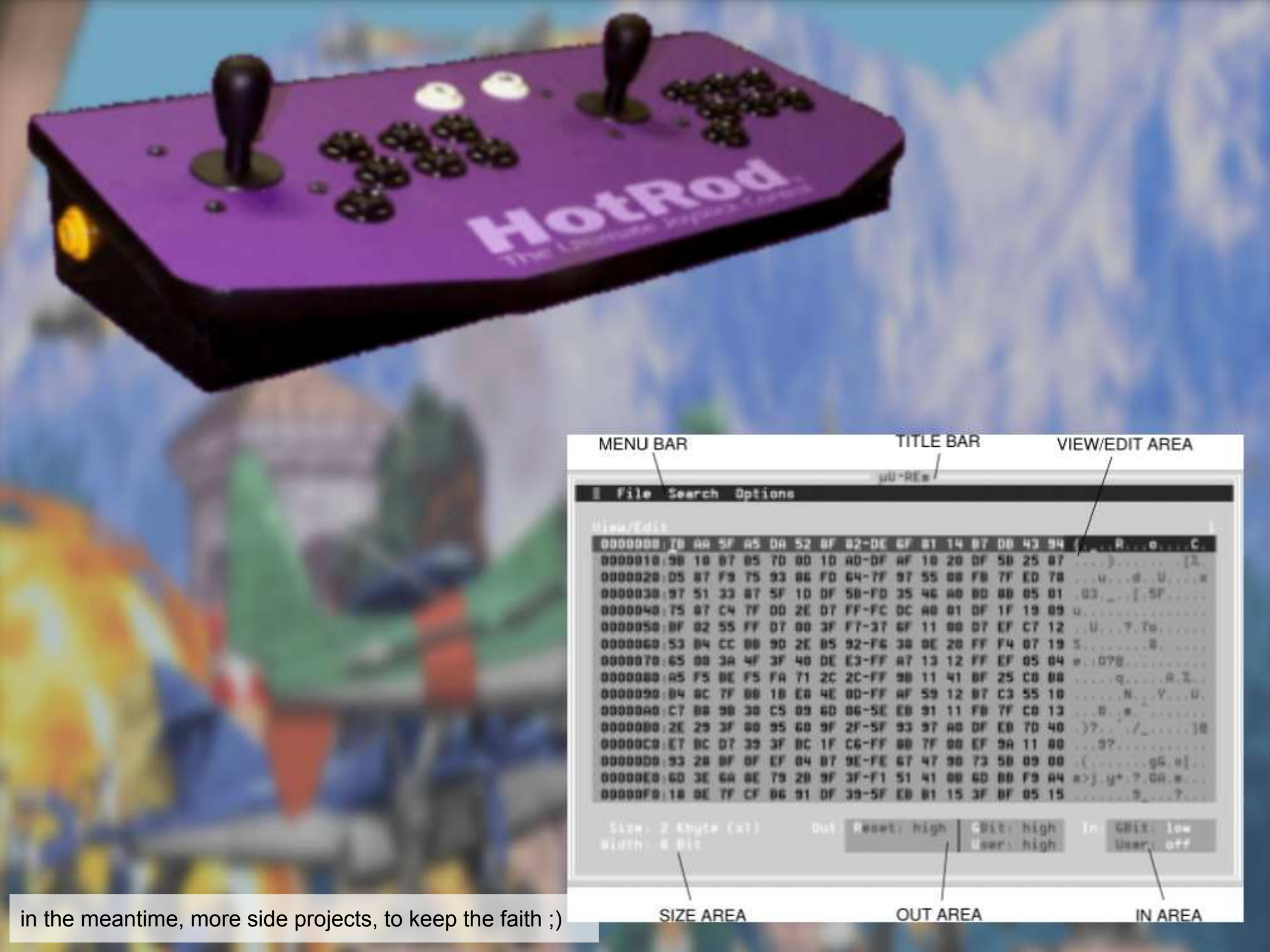
Posted in Business, 8th January 2001 19:44 GMT

A group of gaming enthusiasts called the CPS-2 Shock Team claims to have broken the encryption on the CPS-2 arcade board from Capcom.

While the algorithm itself has not been compromised, the group has managed to extract unencrypted data from the board using the 68k code on the hardware itself, according to a poster on SlashDot. Whether this actually constitutes a break of encryption is a subject under discussion at the aforementioned geek site.

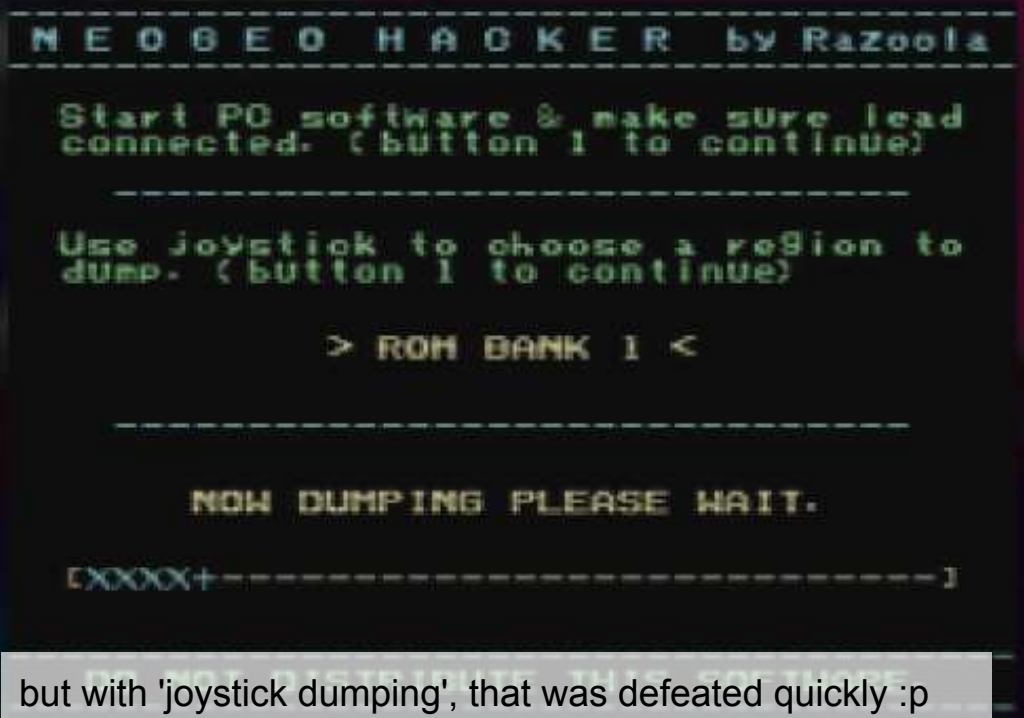
but now emulation was a reality. each game needed to be sent to Raz in a working state.

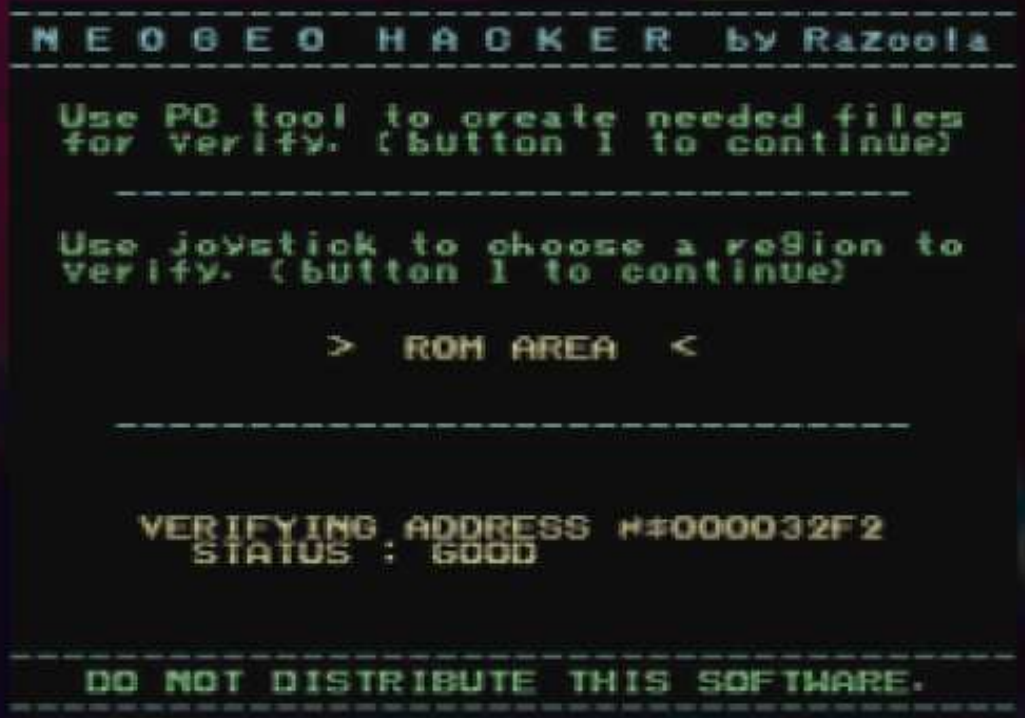
game over for CPS2 ?
not fully. encryption still unknown, no possible restoration yet.



in the meantime, more side projects, to keep the faith ;)


TOTAL
65200
1P
COM
INSERT COIN
45
ROCK HOWARD
KOTARO FUTABA
recent NeoGeo games also featured better protection
CREDIT
00





but with 'joystick dumping', that was defeated quickly :p
(decryption done by Nicola Salmoria)


what about dead CPS2 boards ?
CREDIT 0

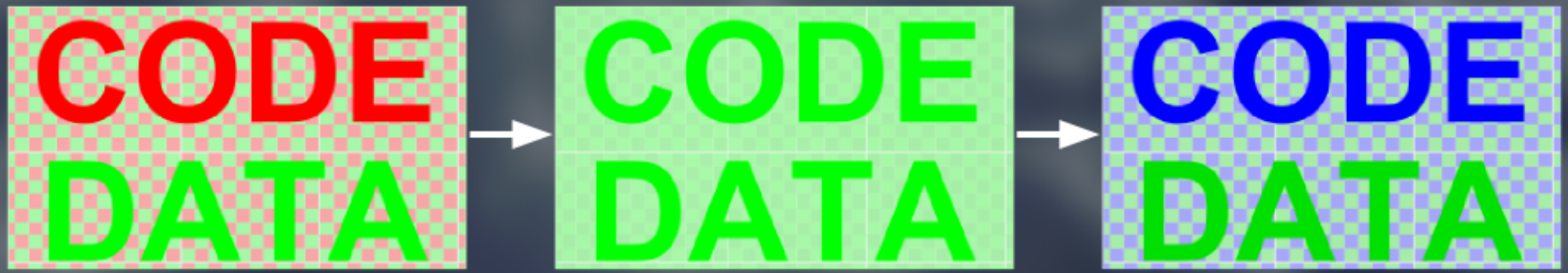
if you put back decrypted code on a dead CPS2,
it still doesn't work.

Razoola was donated a working PCB to sacrifice, then found out why.

```
move.w   #$7000, $400000.l
move.w   #$0, $8040a0.l
move.w   #$807d, $400002.l
move.w   #$1234, $400004.l
move.w   #$0, $400006.l
move.w   #$40, $400008.l
move.w   #$10, $40000a.l
move.w   #$f00, $804040.l
cmpi.l   #$5642194, D0
lea      ($6, PC), A4; ($9d6)
bra      $e82
move.w   #$ffc0, $80010c.l
move.w   #$0, $80010e.l
move.w   #$9000, $800100.l
move.w   #$9080, $800102.l
move.w   #$90c0, $800104.l
```

```
move.w   #$7000, $fffff0.l
move.w   #$0, $8040a0.l
move.w   #$807d, $fffff2.l
move.w   #$1234, $fffff4.l
move.w   #$0, $fffff6.l
move.w   #$40, $fffff8.l
move.w   #$10, $fffffa.l
move.w   #$f00, $804040.l
cmpi.l   #$5642194, D0
lea      ($6, PC), A4; ($9d6)
bra      $e82
move.w   #$ffc0, $80010c.l
move.w   #$0, $80010e.l
move.w   #$9000, $800100.l
move.w   #$9080, $800102.l
move.w   #$90c0, $800104.l
```

video and sound registers had a different address on dead games.
patching these addresses makes them work again !



workflow: decrypt code, merge with data, patch addresses...

Razoola made a universal test ROM,
and 'no more battery' Phoenix versions.


GIGA
MAN 2
THE
POWER FIGHTERS
this also made bootlegs possible.
no more battery...
from MegaMan to Gigaman :(

and also some cool all-in-one:
play all games with just one board.

CPS2, 1994

these 2 games look different...

PC, 1999

CPS2
1994

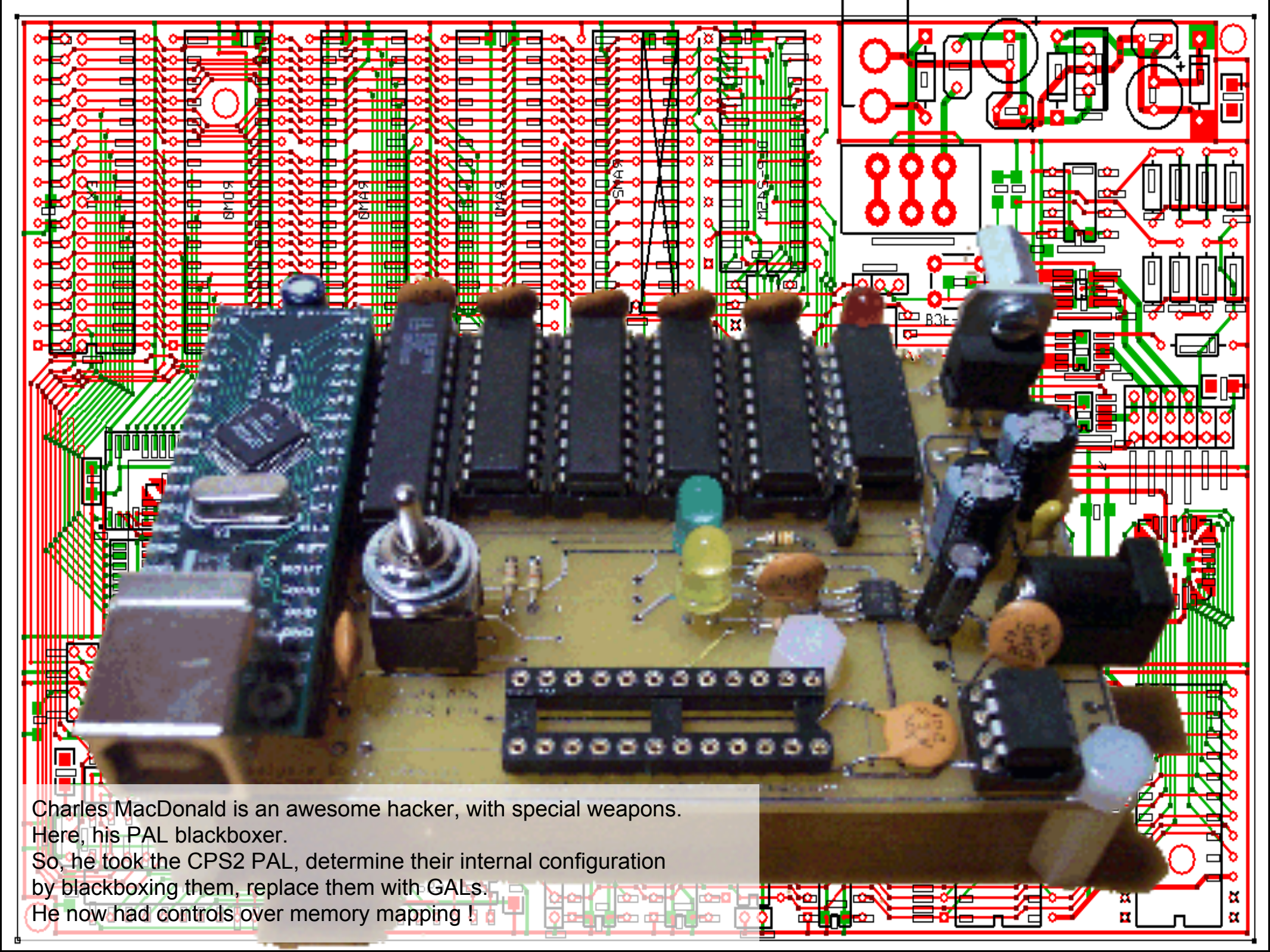
however, the IP was the same.
Some nice lawyer wrote us a letter...
You see who your friends really are,
in these cases ;)

PC
1999

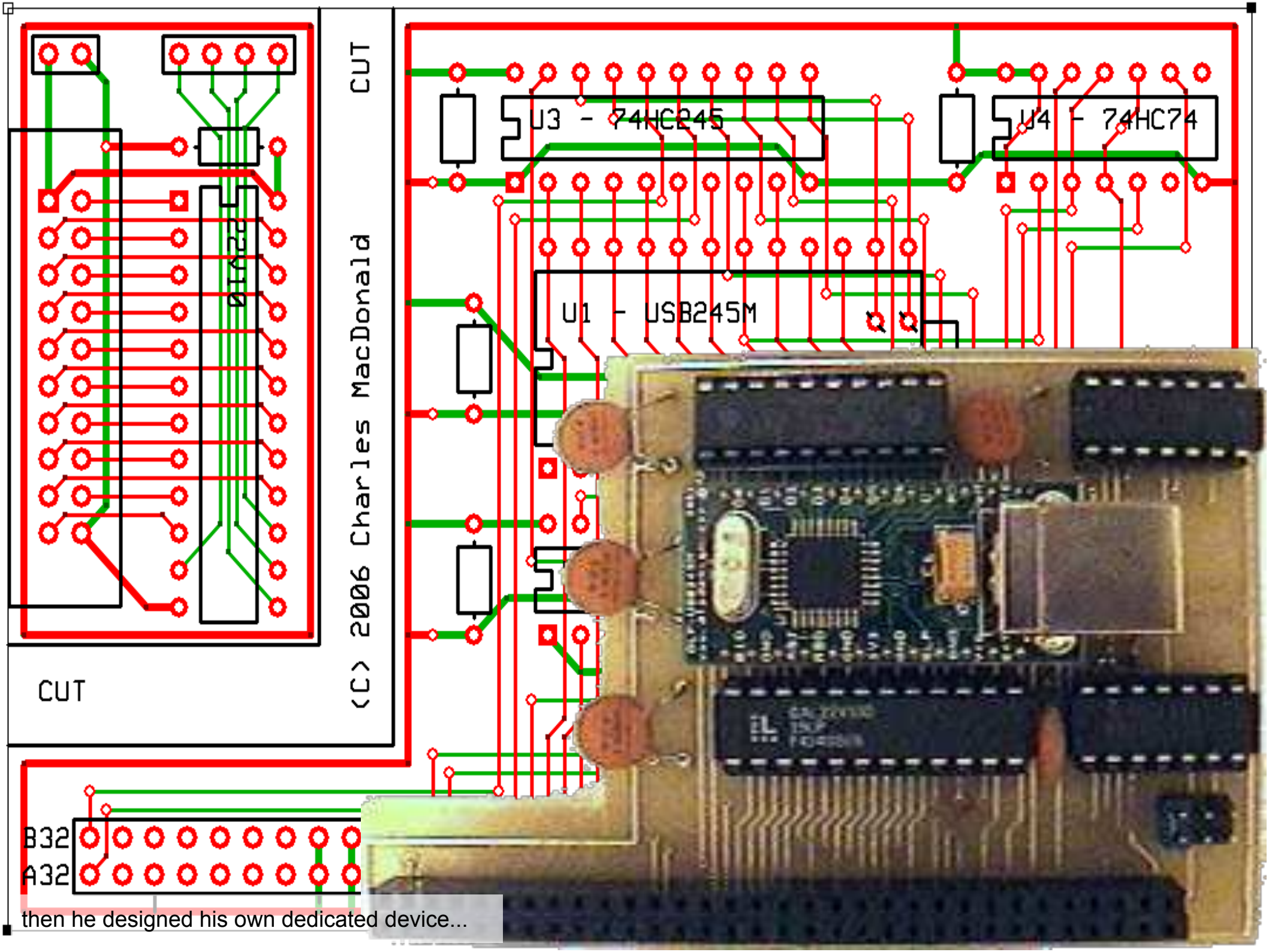
so now even the most obscure CPS2 games were preserved,
but the encryption was still unknown.
and it would take us 200 years to dump all possible values for one game...

so we needed someone else to continue...

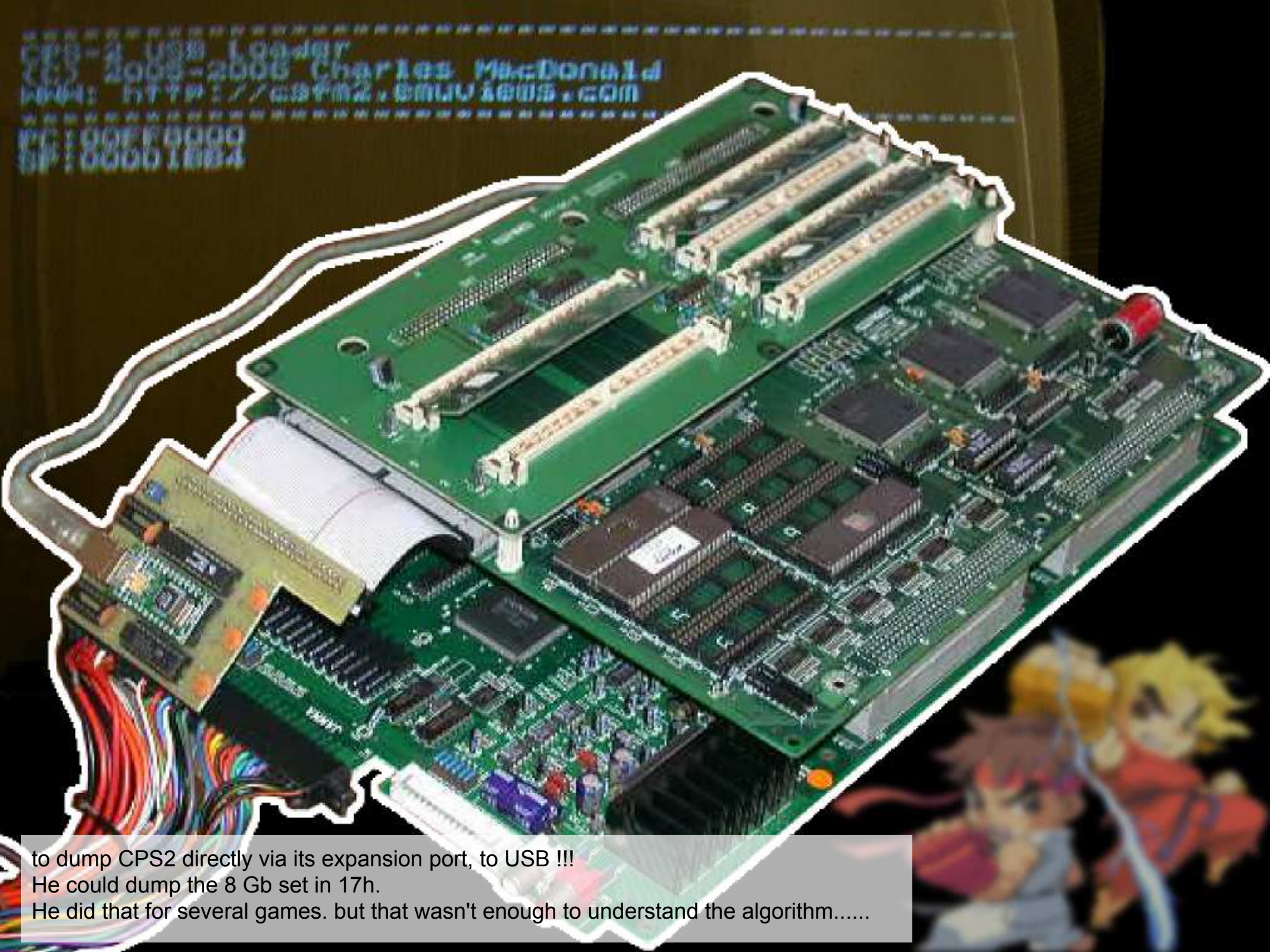
if you can't defeat the ennemy, bring your friends.
In 2005, Charles MacDonald started to work on the CPS2.



Charles MacDonald is an awesome hacker, with special weapons.
Here, his PAL blackboxer.
So, he took the CPS2 PAL, determine their internal configuration
by blackboxing them, replace them with GALs.
He now had controls over memory mapping !

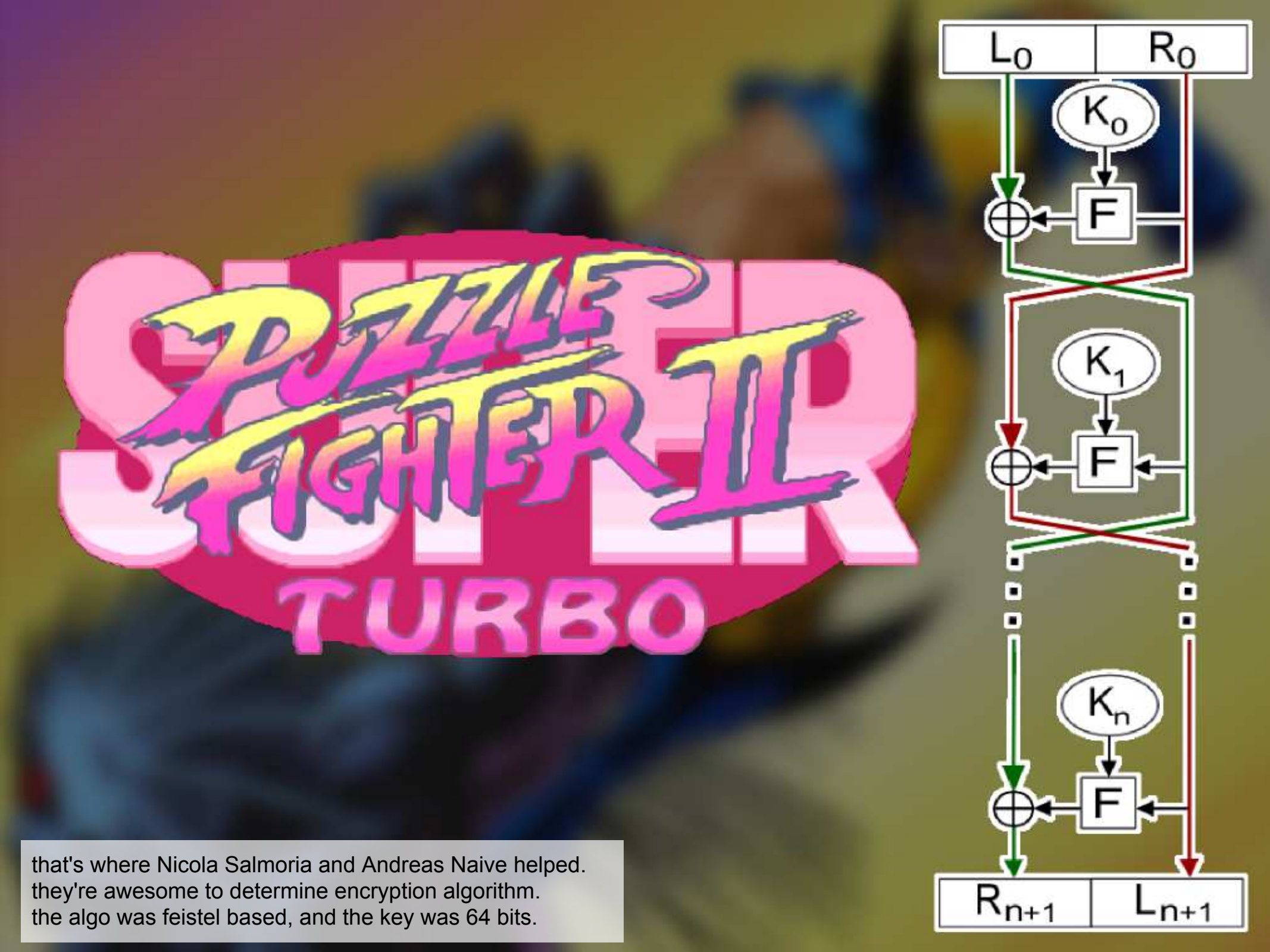


then he designed his own dedicated device...



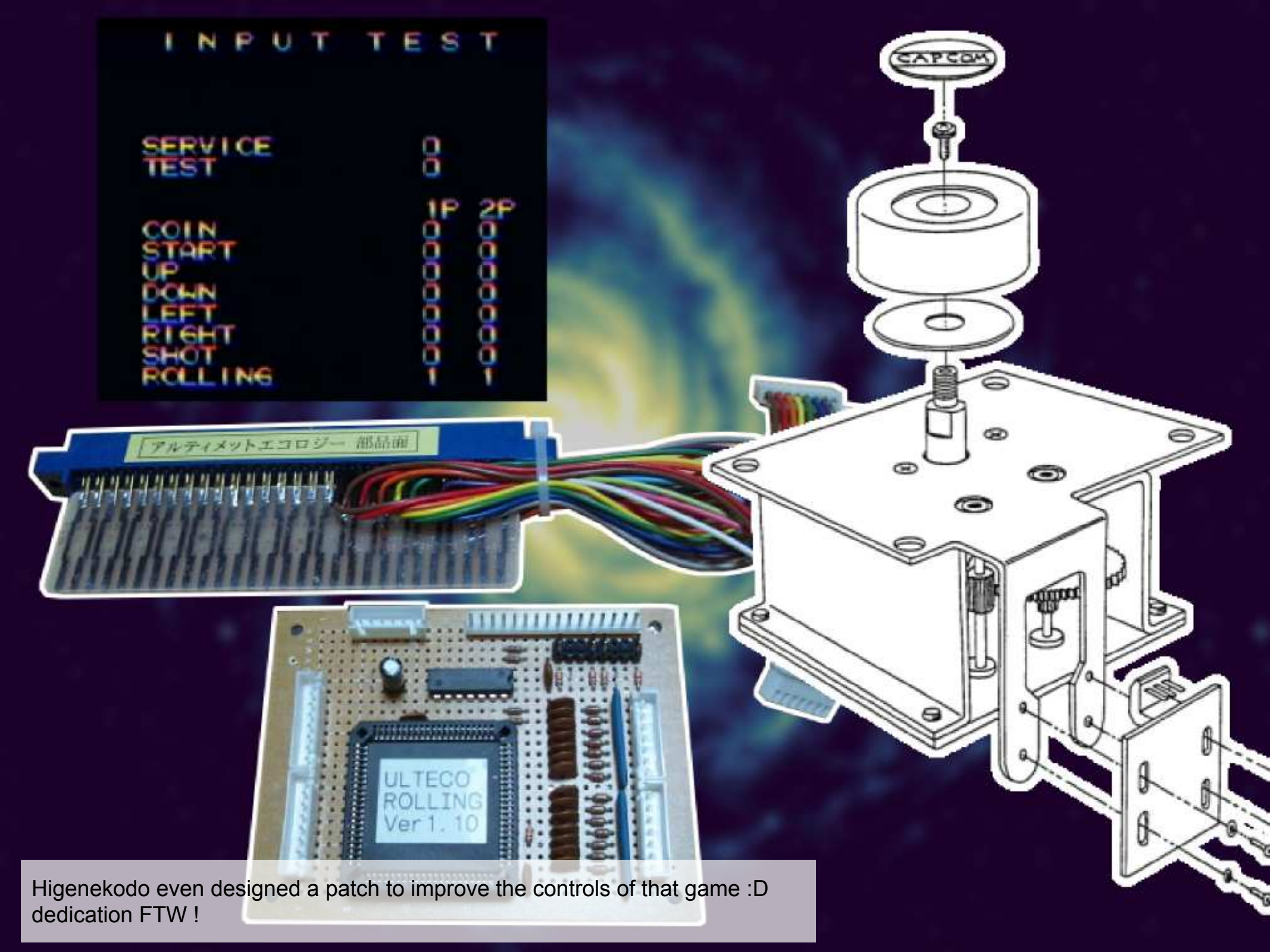
to dump CPS2 directly via its expansion port, to USB !!!
He could dump the 8 Gb set in 17h.
He did that for several games. but that wasn't enough to understand the algorithm.....

so someone else needed to continue to break the algo...

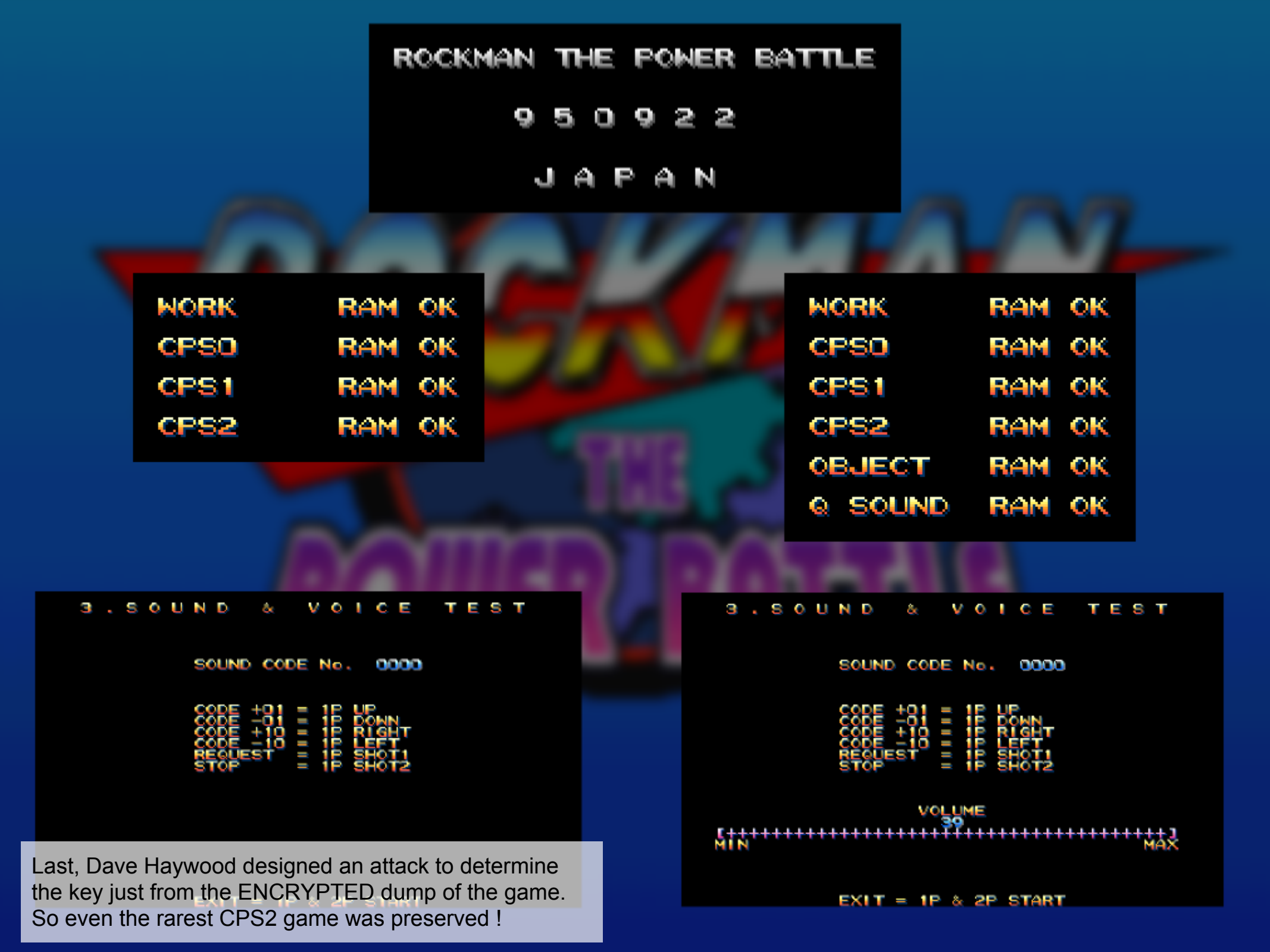


that's where Nicola Salmoria and Andreas Naive helped.
they're awesome to determine encryption algorithm.
the algo was feistel based, and the key was 64 bits.

so, from one european decrypted dump of a game,
the key could be determined,
which could then decrypt the rare japanese version of the game.

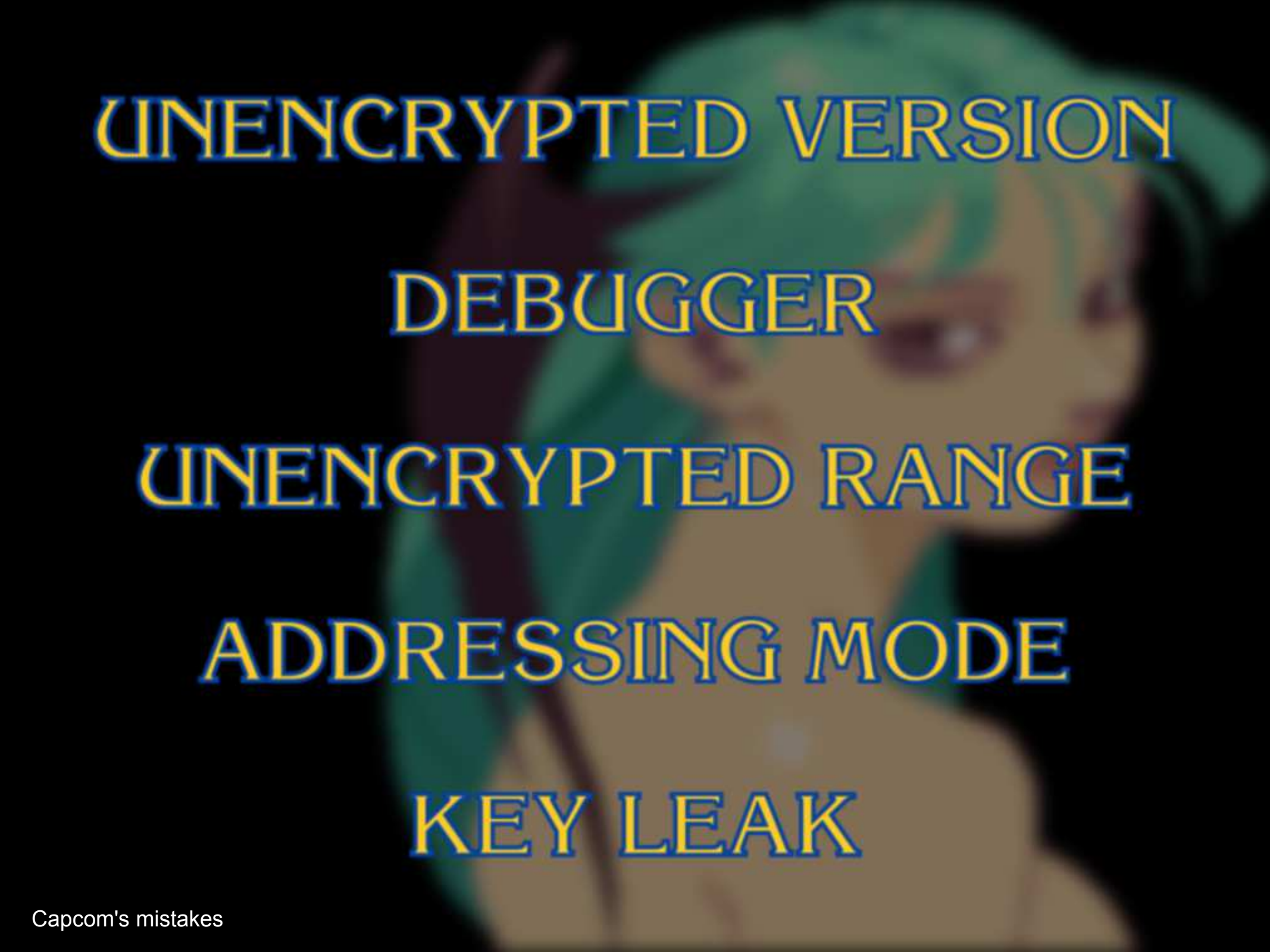


Higenekodo even designed a patch to improve the controls of that game :D dedication FTW !



Last, Dave Haywood designed an attack to determine the key just from the ENCRYPTED dump of the game. So even the rarest CPS2 game was preserved !


~ Epilogue ~



Capcom's mistakes

CLUMSY HACKS

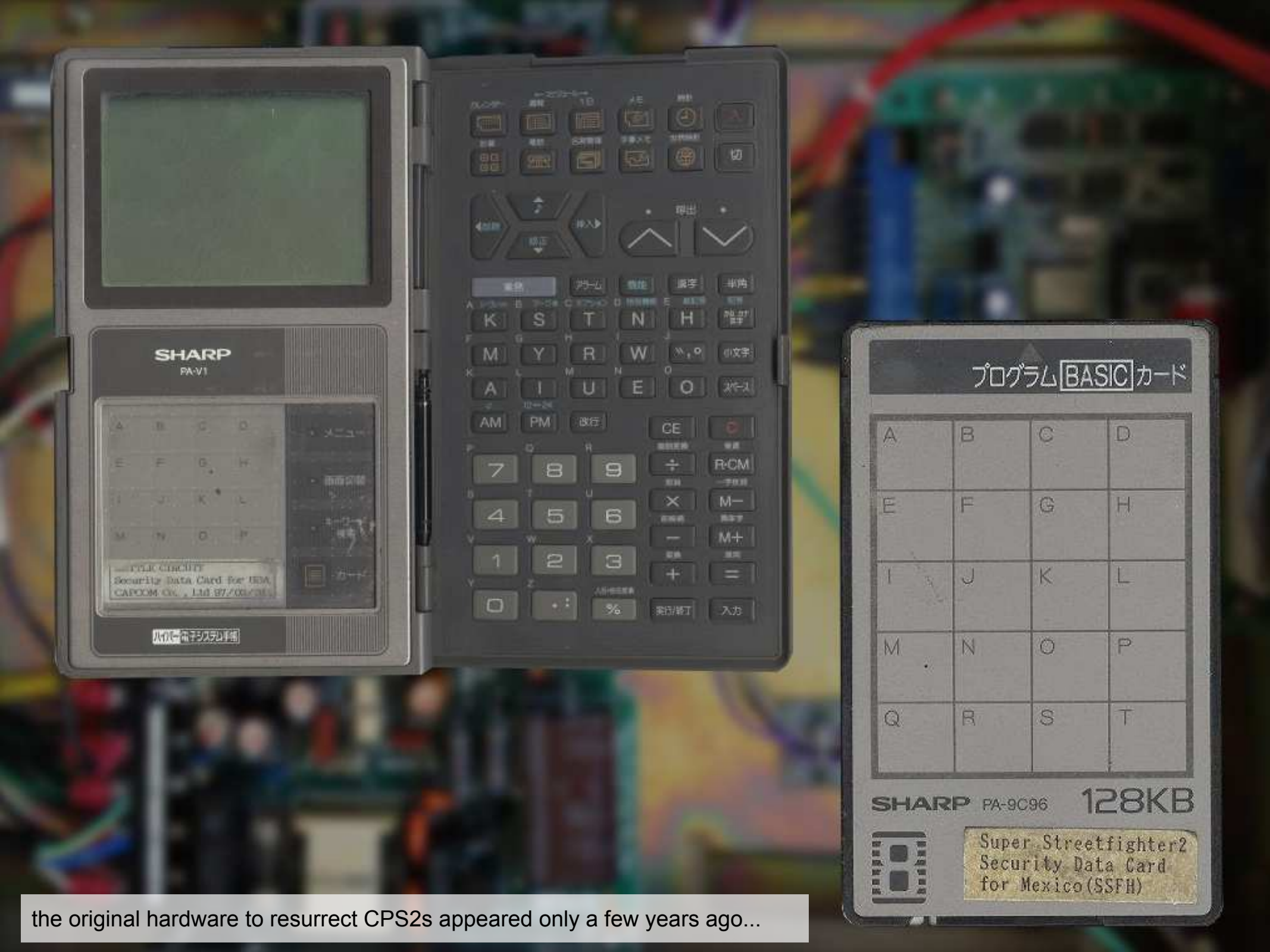
JOINT EFFORT

MANY CONTRIBUTIONS

SUCCESS

many people contributed, in various ways

and overall, an awesome victory !

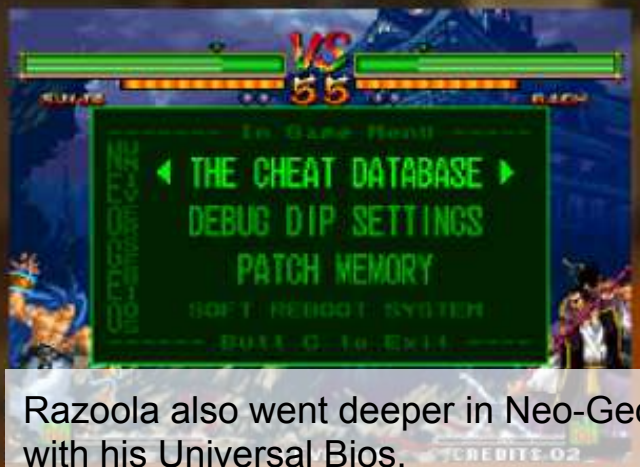


the original hardware to resurrect CPS2s appeared only a few years ago...

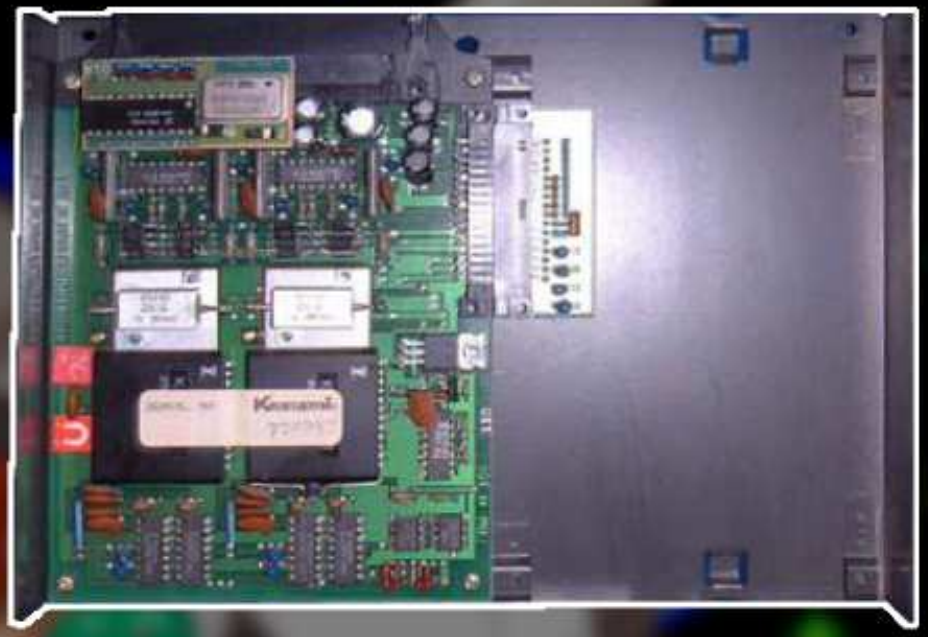
CPS2's protection is seen as related to Sega Naomi's

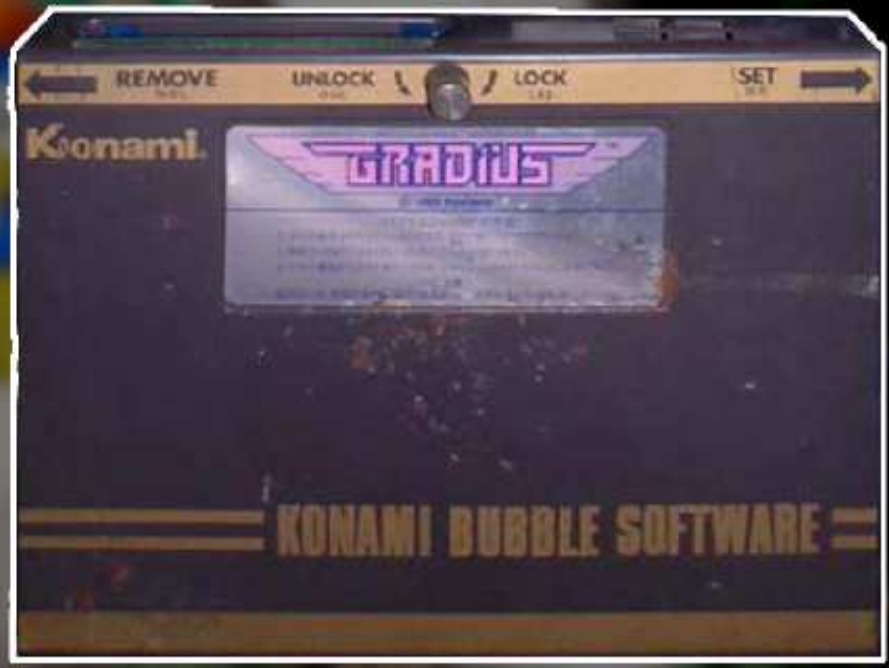

```
REWRITE GAME MENU BY *DARKSOFT* Ver 1.00
          > 1. SFIII NEW GENERATION
            2. WARZARD / RED EARTH
            3. JOJO'S VENTURE
            4. JOJO'S BIZ. ADV.
            5. SFIII 2ND IMPACT
            6. SFIII 3RD STRIKE A
            7. SFIII 3RD STRIKE B
```

Andreas Naive later defeated CPS3 encryption
Then recently, Darksoft resurrected them and made an all-in-one CPS3 CD !



Razoola also went deeper in Neo-Geo enhancing, with his Universal Bios.





this is the Bubble Memory system.
it's **very** fragile.

to work, it needs to warm up to a certain temperature.
to me, this big countdown says:
'all these games are going to disappear if no one hacks or contribute for them'

Razoola's CPS2Shock
http://www.cps2shock.com
http://web.archive.org/web/*/http://cps2shock.retrogames.com

Charles MacDonald's Home Page
http://cgfm2.emuviews.com/old2005.php

Nicola Salmoria's MAME Ramblings
http://mamelife.blogspot.com/2006/01/8gb-2-is-still-4gb.html
Andreas Naive's Notas de Andy
http://andreasnaive.blogspot.com/2006_12_01_archive.html
Mame's CPS2 encryption source
http://mamedev.org/source/src/mame/machine/cps2crpt.c.html

DarkSoft's Breaking CPS3
http://64darksoft.blogspot.com

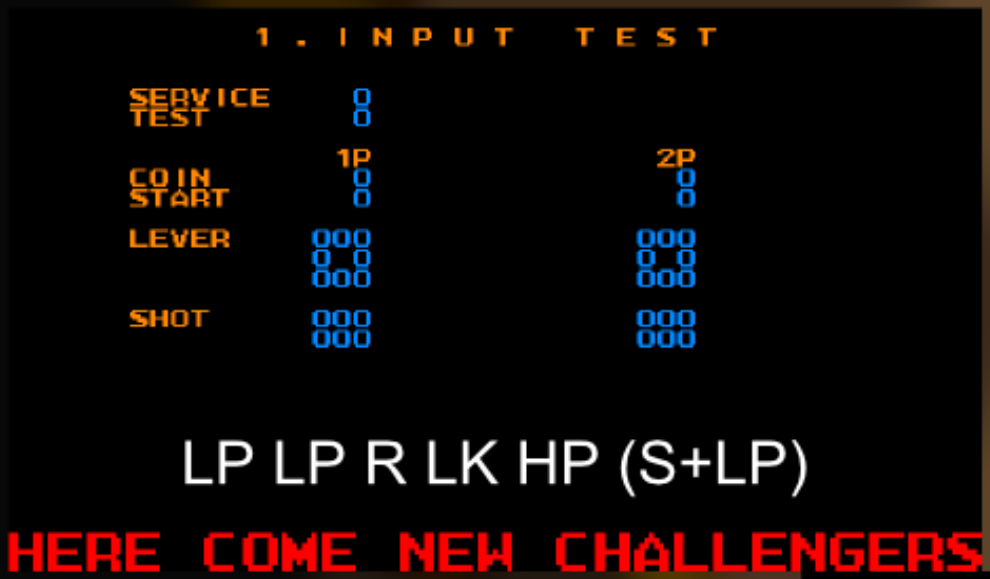
(links)

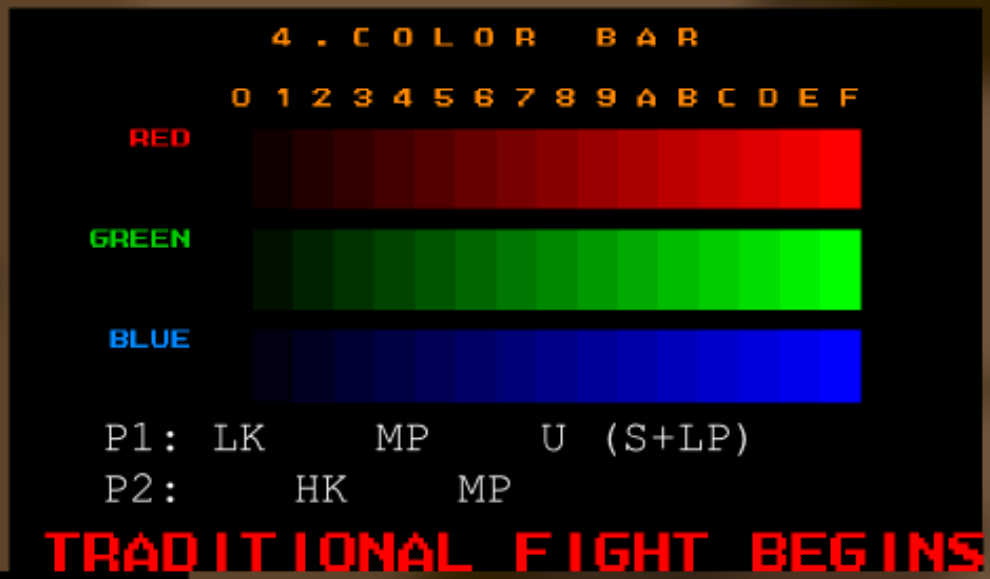
yes, this is a CPS2 timeline :p

some bonus ?

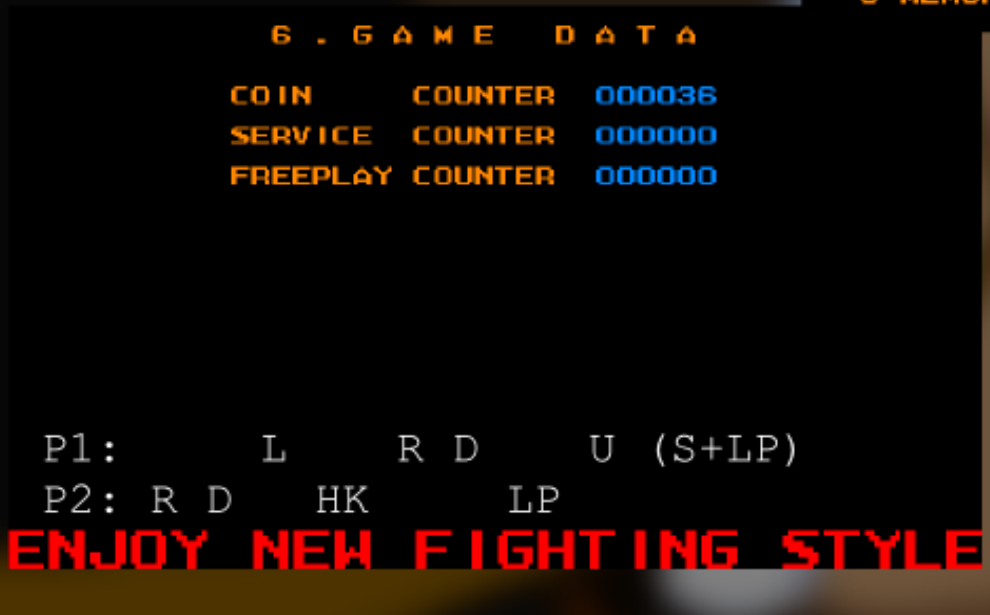
SFA3 has a time lock: if you let it run long enough,
some special modes are unlocked.
the title background tells how many modes are unlocked.

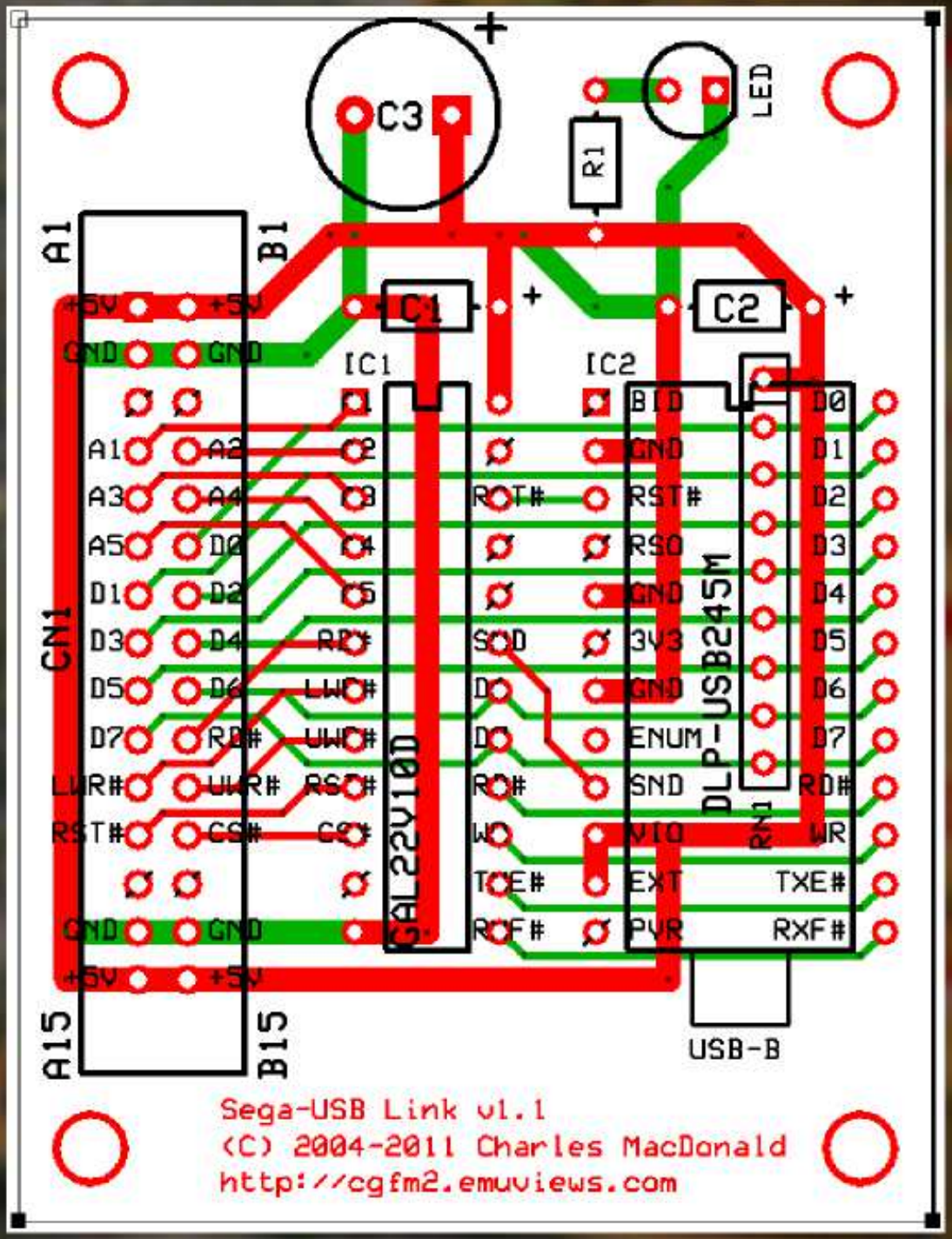
extra characters, extra playing modes

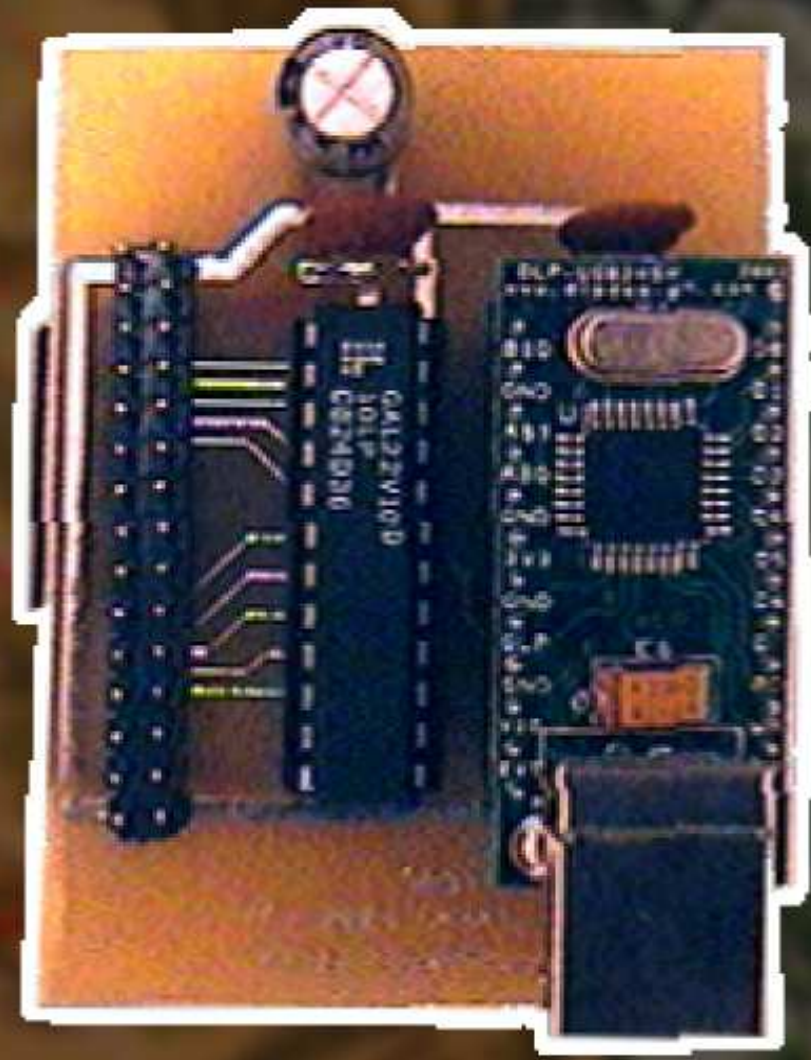




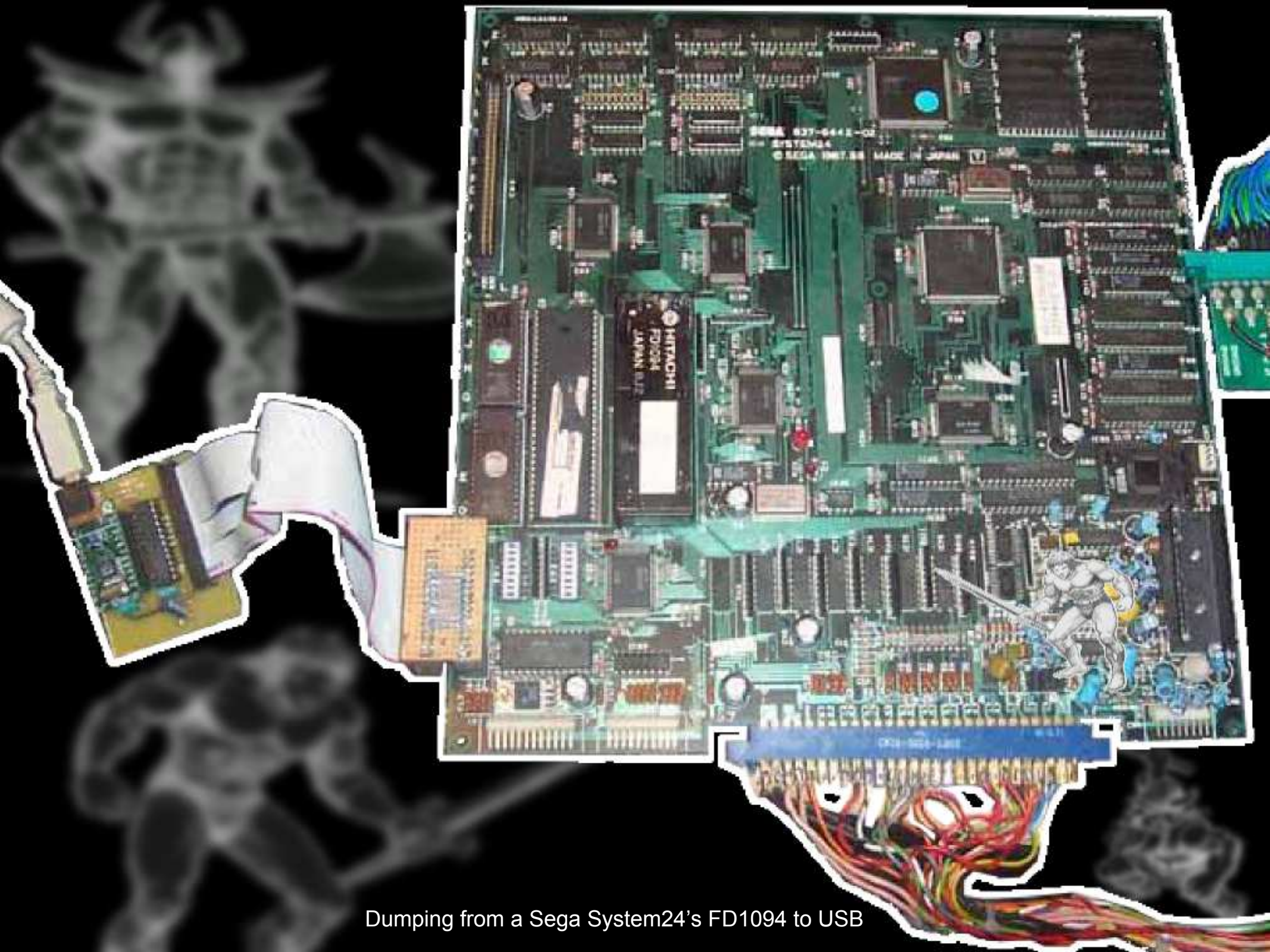
Hidden in the operator menu, Razoola found the crazy cheat codes in the disassembly to turn on this extras without waiting weeks.







Charles MacDonald also worked on Sega hardware and created his own device for it...

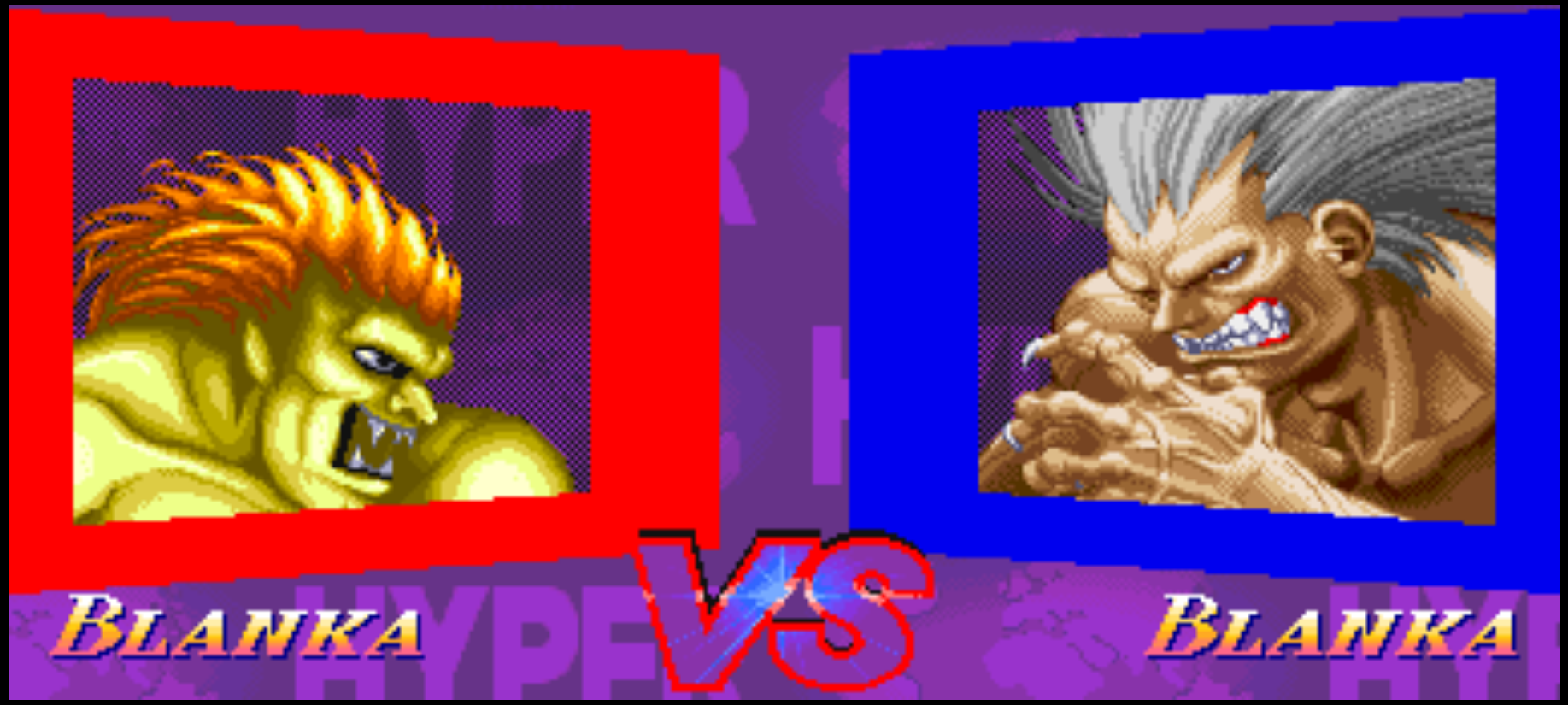


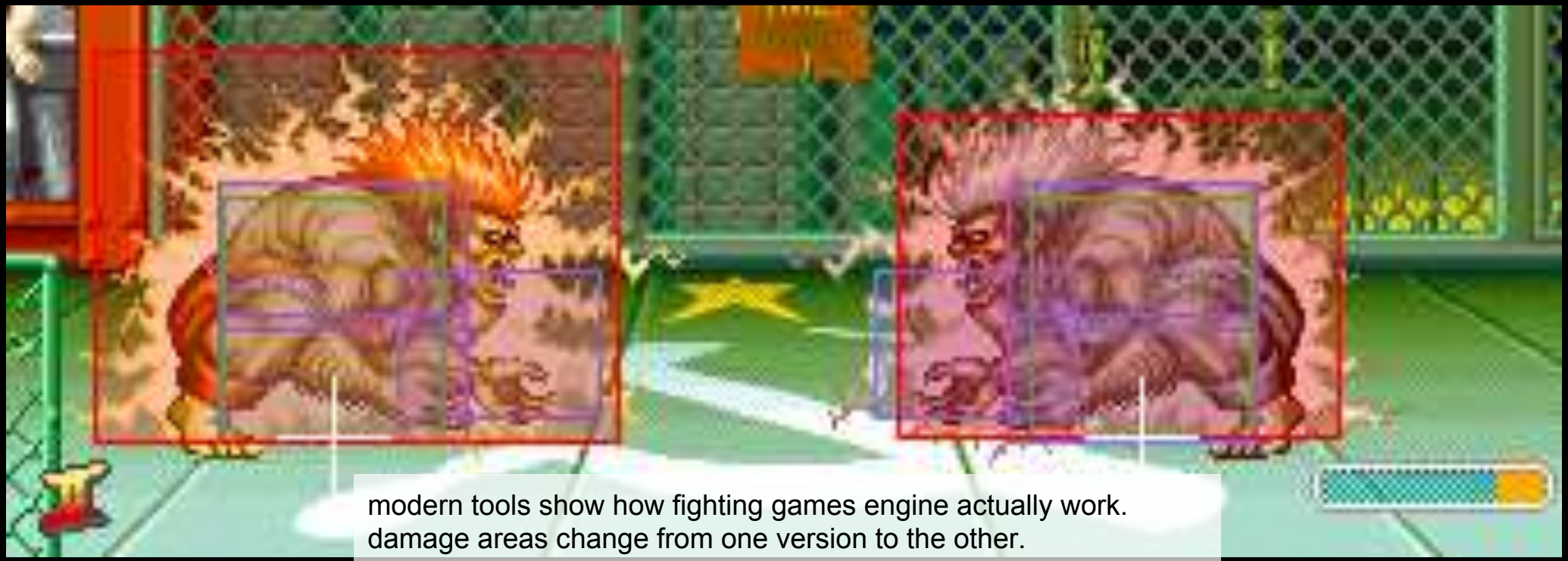
Dumping from a Sega System24’s FD1094 to USB

to preserve games from
System 16, 24 & System X


Last Survivor
Last Survivor, a System X game from 1989,
was thought to be lost forever.
Someone still had one in working conditions:
it was preserved, 20 years later !
SEGA
©SEGA 1989

it's a split-screen multiplayer FPS





modern tools show how fighting games engine actually work.
damage areas change from one version to the other.

there are bugs in the official releases !

attack behind you, or be hit for no reason...

tools assisted speedruns abuse games
via standard controls.


The End . . . ?