Opening Electronic safe locks with Ketchup & Lasers

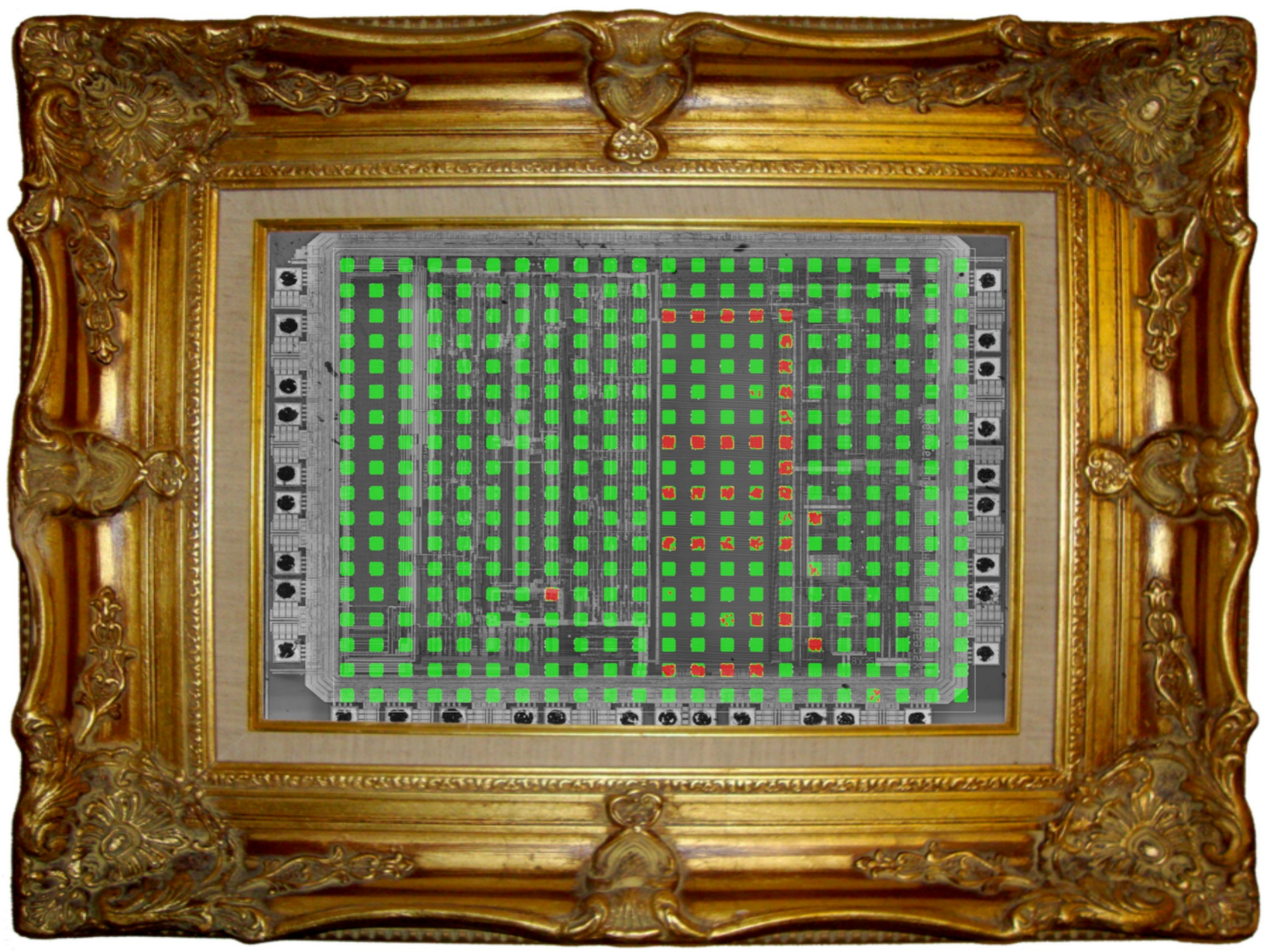
9th of February

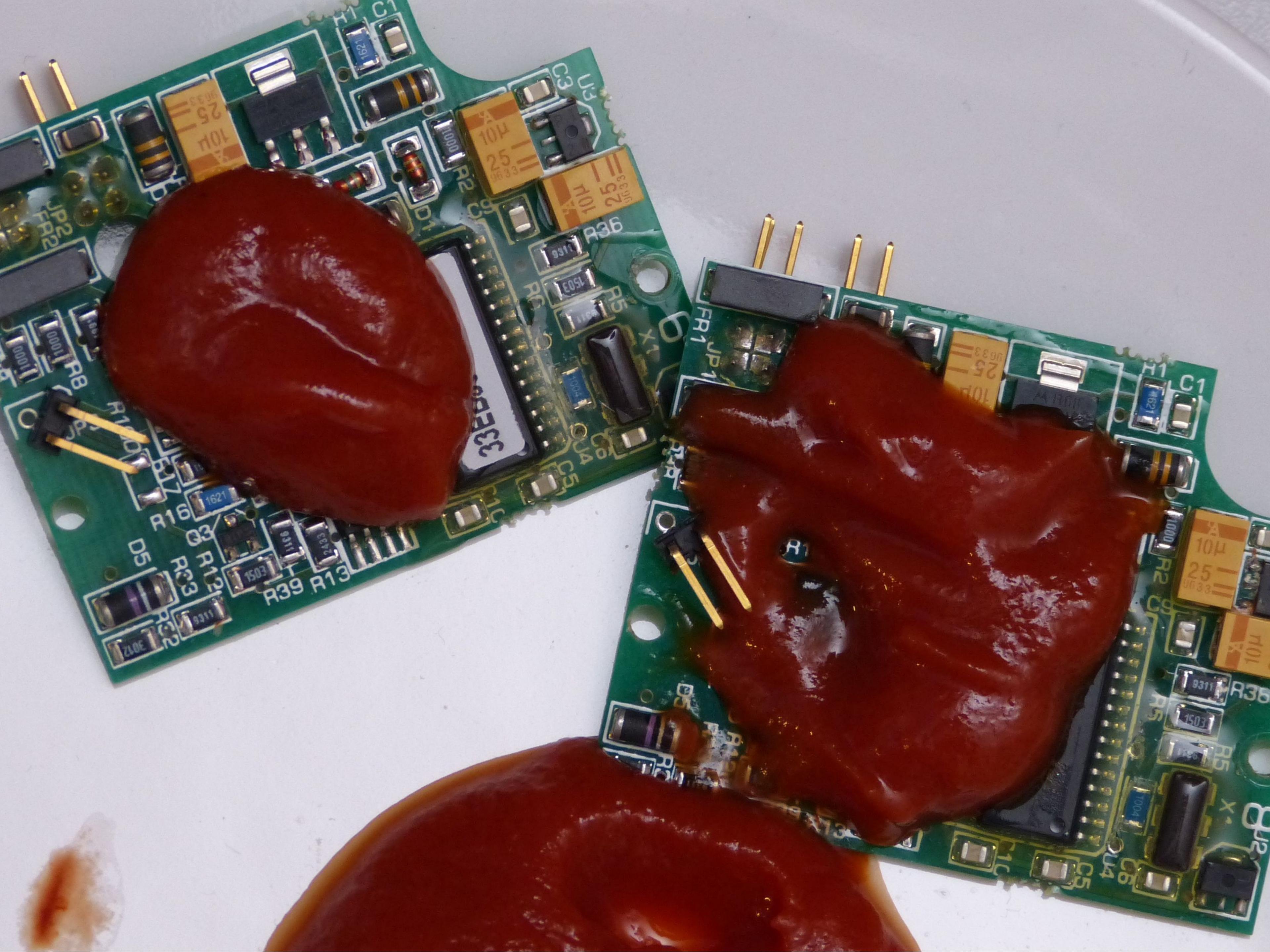
Hackerhotel 2024

Jan-Willem Markus


dormakaba
LOCKED
15:14
Enter
Mode
DEL
0
1
2
3
4
5
6
7
8
9


4 3 3 2 9 3 2 3 D 6 0 2 A
dormakaba
RoHS
COMPLIANT
2002/95/EC
Type: Axessor USB
Part No.: 3582701302
Serial No.: 43329 323D6 02A
Version: 91700.27 2018
VdS 2396 Kl.2 M102413
EN 1300 Class B
VdS
SECURITY
LISTED
High-security Electronic
Lock Type1 4R95
Manufacturer 100530-733
Input Unit
Power Supply
X1
X2
IN2
GND
IN1+
IN1-
OUT1
OUT2





R1
C1
C3
U3
10µ
25
R2
C9
R36
D1
R6
R5
X1
C6
U4
C5
R16
Q3
R12
R13
R39
R33
R32
D5
JP2
FR2
R8
FR1
JP1

Whois Jan-Willem Markus

riscure

- Work:
  - Electronics engineering
  - Security analyst & trainer at Riscure
  - Advanced hardware attacks
- Locksport:
  - President of The Open Organisation Of Lockpickers (Toool)
  - Lockpicking workshops
  - Sharing knowledge on Toool Blackbag
  - Research: Whatever has my interest
- Contact
  - Jan-Willem@Toool.nl
  - @jwrm22

riscure

Electronic safe locks

Introduction

Electronic safe locks

- Electronic safe locks are interesting:
  - Small attack surface
  - Standalone
  - Good basis for security
  - Hardware attacks
  - Quite affordable (usually)

Electronic safe locks

- Force multiplication
- Secure by design

Safe Door

Electronic safe locks

- Consumer / commercial
  - Requirements:
    - UL 2058 Type 1
    - Easy to use
    - Reliable locks for a good price

Electronic safe locks

- Banking and Pharmacy
  - Requirements:
    - Multi user
    - Auditing
    - Delays
    - 2FA

Electronic safe locks

- Government special
  - Requirements:
    - FF-L-2740 B
    - EMP proof
    - TEMPEST proof
    - Etc
  - Kaba Mas X0 series
    - X07: 1992
    - X08: 1998
    - X09: 2002
    - X10: 2013


INSTALLA
INSTRUCTI
MODEL X-09 ®
HIGH SECURITY ELECTRONIC LOCK TYPE FF-L-2740A
S/N: X09SR0140711062012ARM
COVERED BY U.S. AND FOREIGN PATENTS. OTHER PATENTS PENDING
KABA MAS LLC
LEXINGTON KY U.S.A.

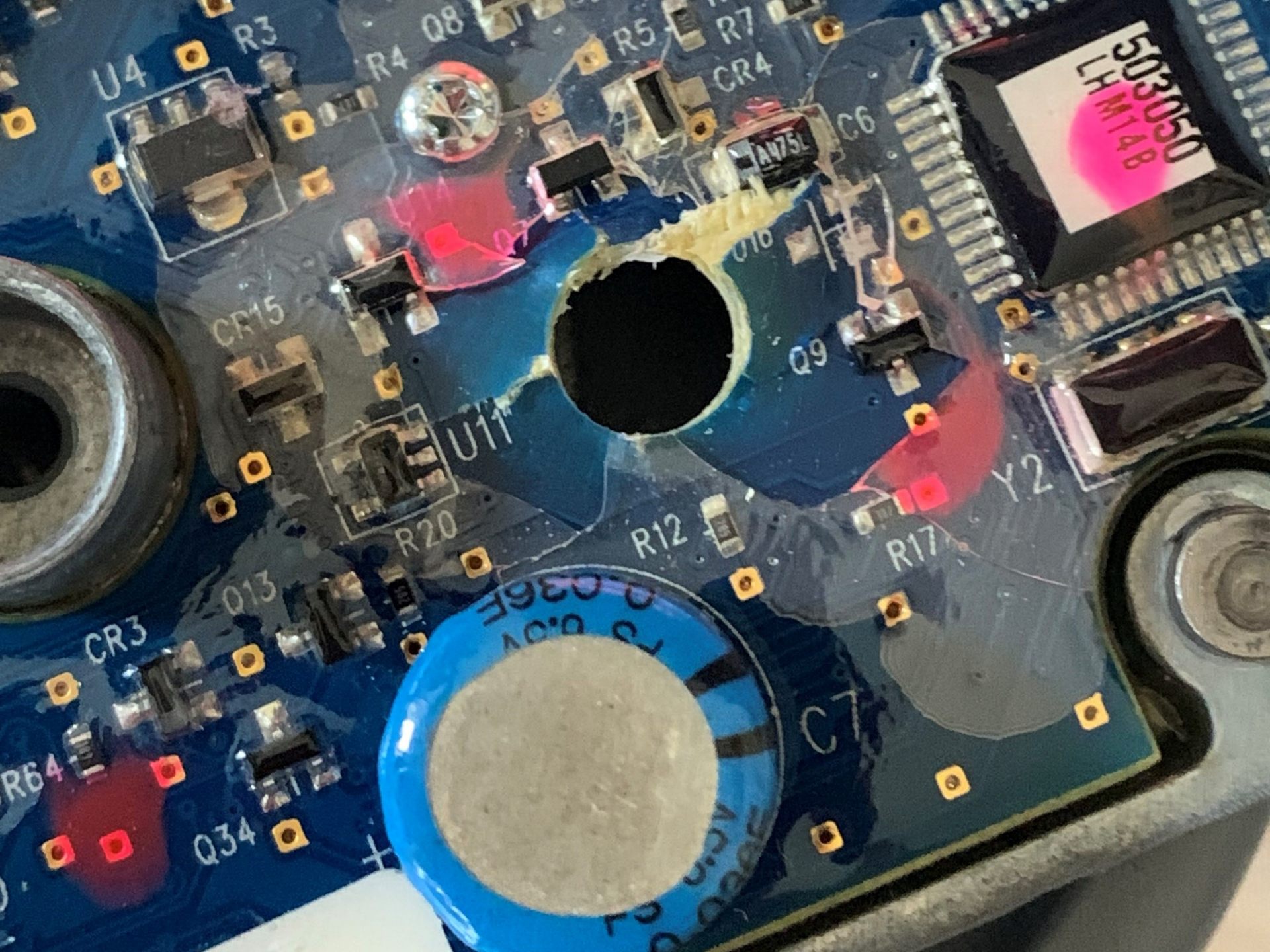
riscure

Novel work on the X0 locks

Access to samples

Samples from the USA

- eBay bulk
- Trade with fellow lockpickers
- Shipping cost is bottleneck


U4
R3
R4
Q8
R5
R7
CR4
C6
5030S0
LH M14B
CR15
U11
Q9
R20
R12
Y2
R17
Q13
CR3
C7
R64
Q34

Hardware Reverse engineering

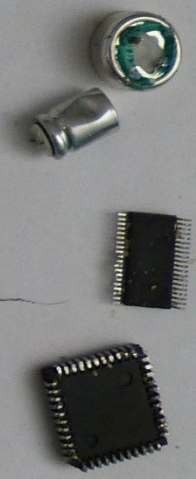
Hardware Reverse Engineering (HWRE)

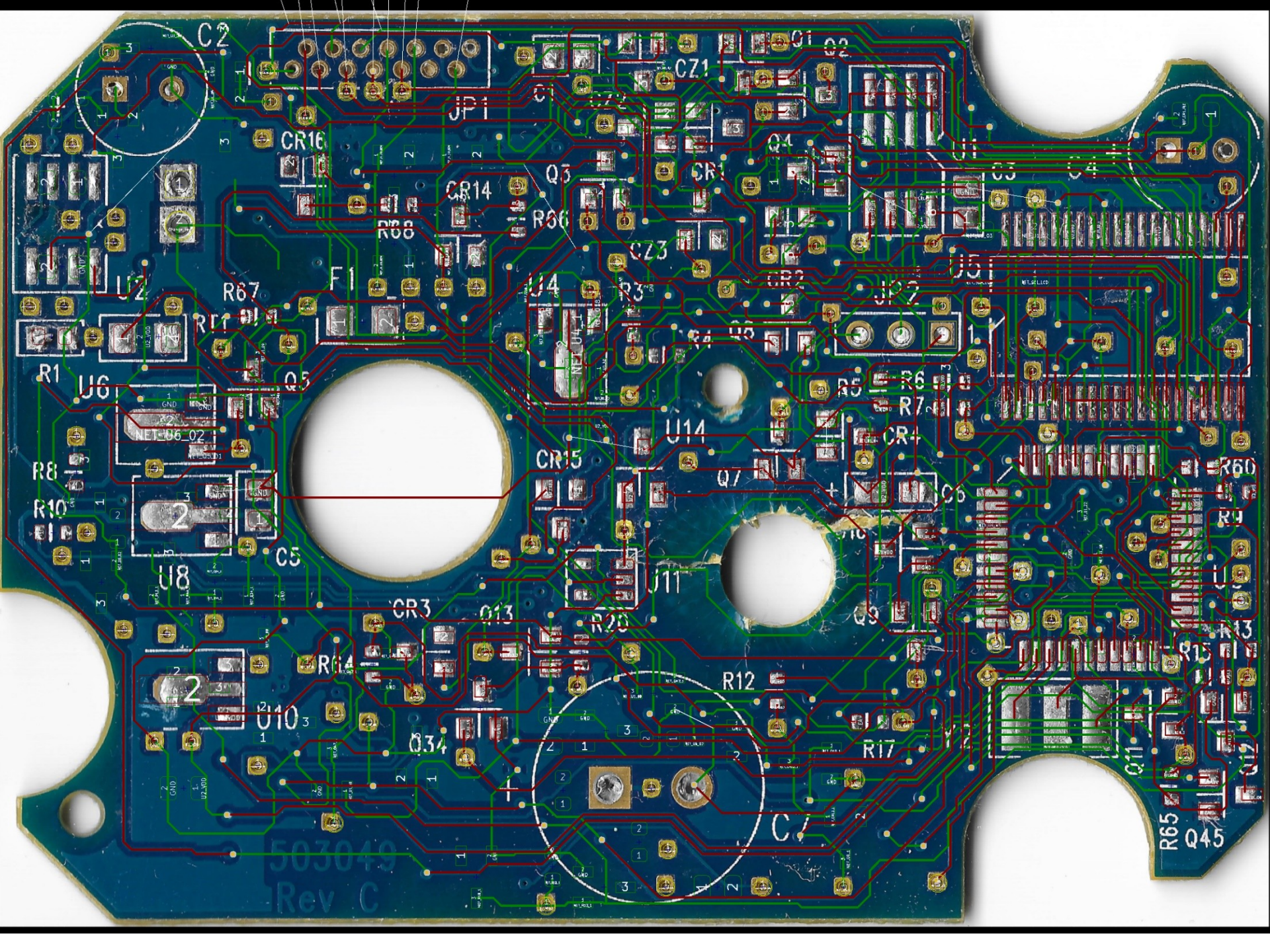
- Taking the lock a part
- Determining the function of each part
- Create a schematic

- Focused on all the X0* at the same time → Slow progress


BAKU 858D
350
DIGITAL
SKYTRONIC

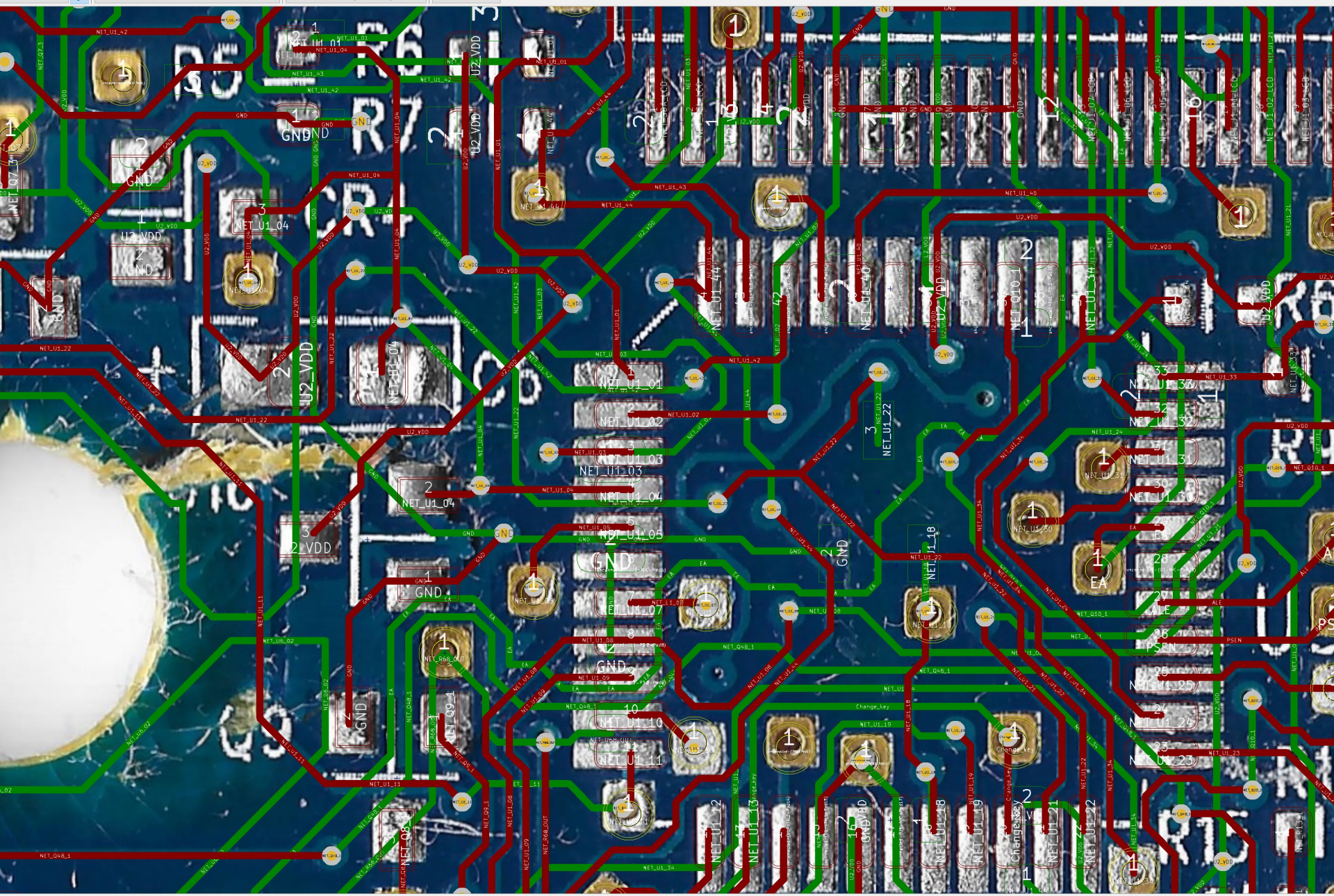
	1	2	3	4	5	6	7	8	9	10
A	F2	CR2	CR4	CR3	CR1	R23	R21	CR10	Q8	Q15
	Q17	Q18	CR9	CR8	R22				U6	U4
	Y1	C4 C13 C14 C18	U1	U8	U7	R14	CR7	CR6	Q2	Q3
							U5	U9	P1	RT1
	C16	FB1	R20	R19	C9	CR12	R39	R30	R38	C44 15
	Q14	R31	Q13	Q12	R17	Q10	Q15	Q14	FB2	C17
	Q9	R26	R18	Q16	R32	R13	R25	CR13	C3	R1
	R3	Q1	C12	R24	Q7	CR11	C21	R35	R36 2	C11




C2
JP1
CR16
CR14
R88
Q5
R56
CZ1
CZ3
U4
R3
F1
R67
U2
R1
U6
R8
R10
U8
C5
CR15
U14
Q7
CR4
R5
R6
R7
C6
R60
R9
U11
CR3
Q13
R20
Q9
R13
R15
R14
U10
Q34
R12
R17
C7
R65
Q45
503049
Rev C

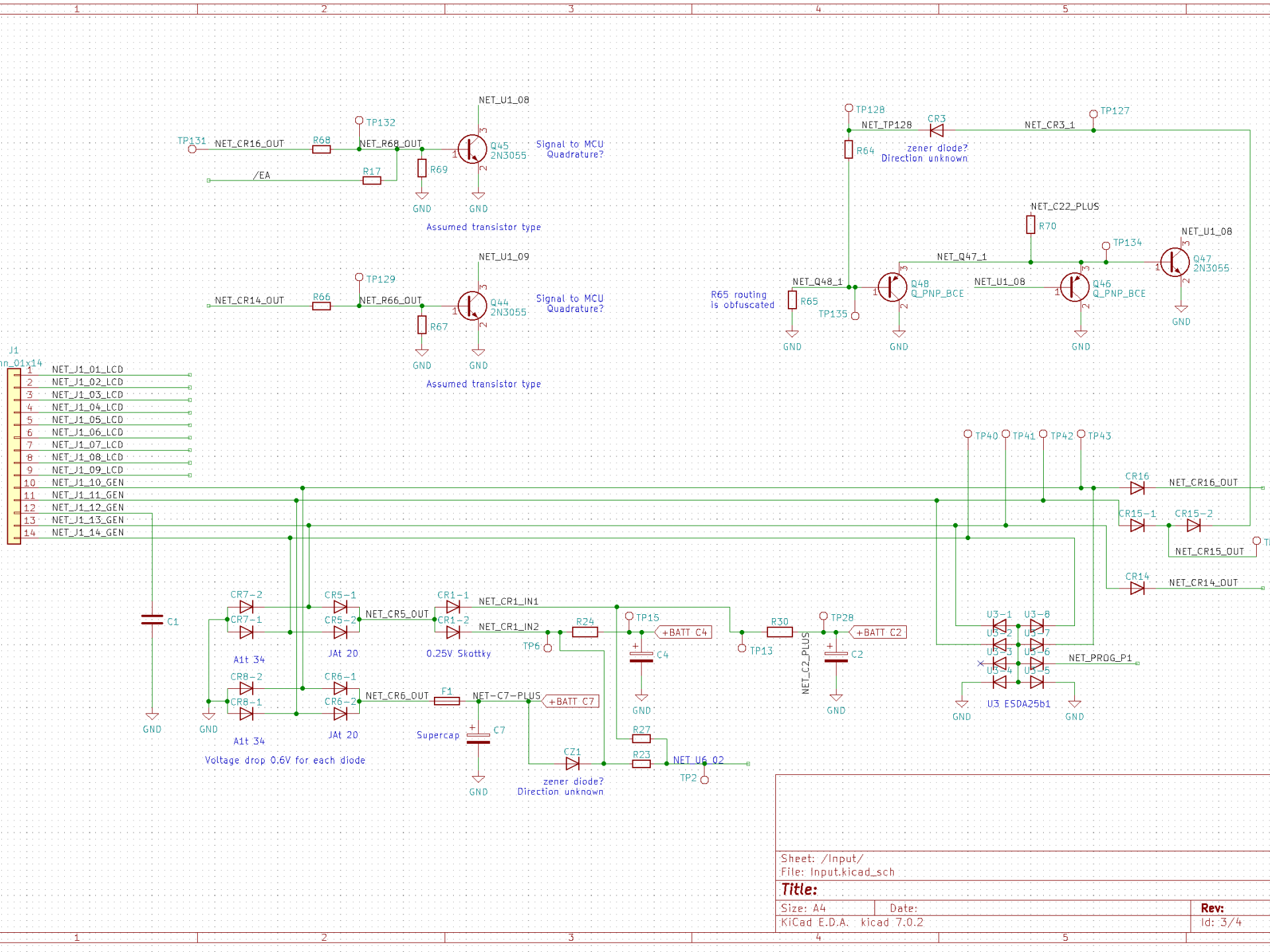
- PCB Editor

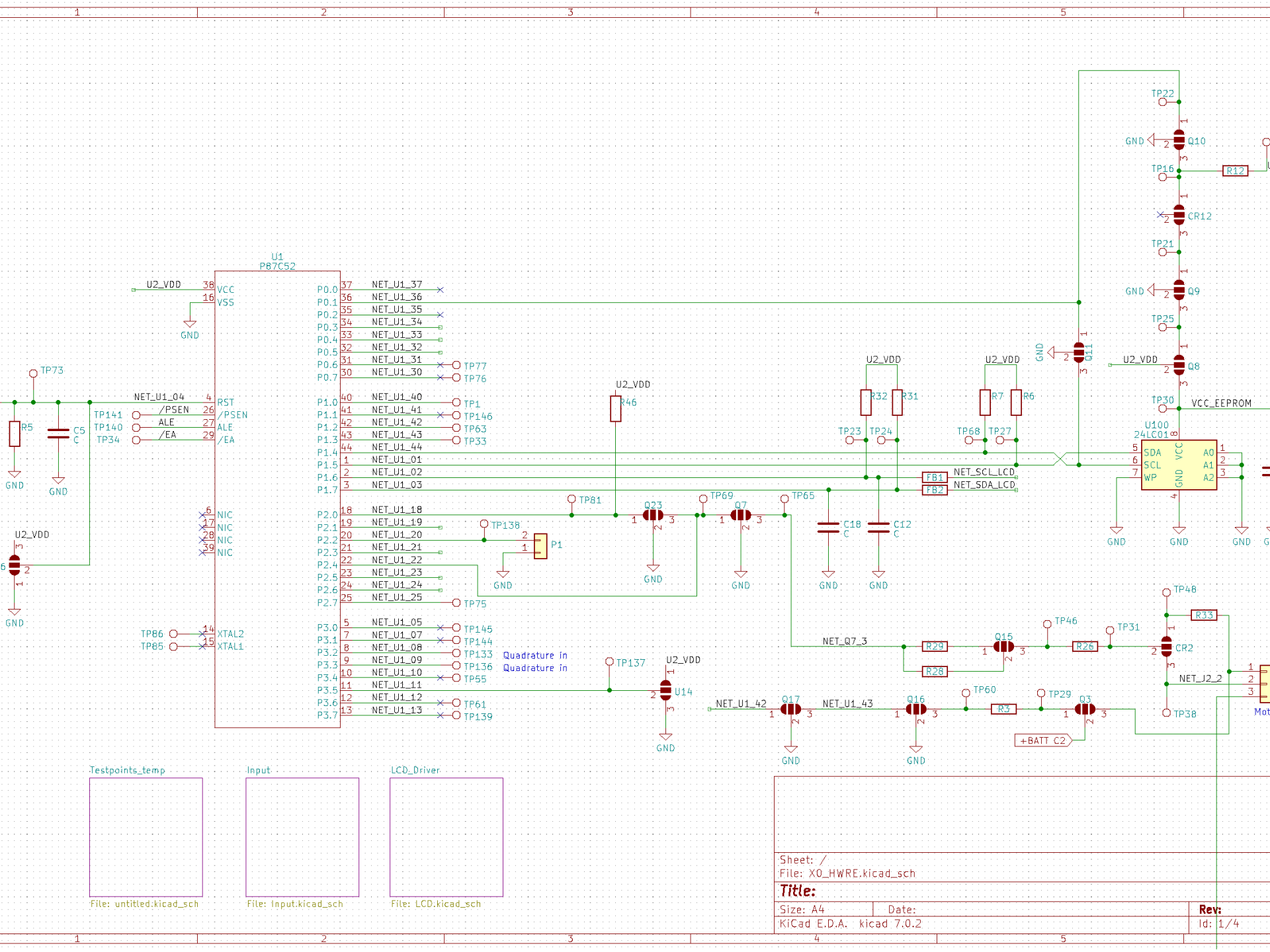
Place Route Inspect Tools Preferences Help



Track Segments	Nets	Unrouted
2640	128	21

Z 27,53 X 147,4470 Y 83,8200 dx 147,4470 dy 83,8200 dist 169,6066


NET_U1_08
TP132
TP131
NET_CR16_OUT
R68
NET_R68_OUT
Q45
2N3055
Signal to MCU
Quadrature?
/EA
R17
R69
GND
GND
Assumed transistor type
NET_U1_09
TP129
NET_CR14_OUT
R66
NET_R66_OUT
Q44
2N3055
Signal to MCU
Quadrature?
R67
GND
GND
Assumed transistor type
TP128
NET_TP128
CR3
NET_CR3_1
TP127
R64
zener diode?
Direction unknown
NET_C22_PLUS
R70
TP134
NET_U1_08
Q47
2N3055
NET_Q47_1
NET_Q48_1
Q48
Q_PNP_BCE
NET_U1_08
Q46
Q_PNP_BCE
R65 routing
is obfuscated
R65
TP135
GND
GND
GND
GND
J1
Conn_01x14
1 NET_J1_01_LCD
2 NET_J1_02_LCD
3 NET_J1_03_LCD
4 NET_J1_04_LCD
5 NET_J1_05_LCD
6 NET_J1_06_LCD
7 NET_J1_07_LCD
8 NET_J1_08_LCD
9 NET_J1_09_LCD
10 NET_J1_10_GEN
11 NET_J1_11_GEN
12 NET_J1_12_GEN
13 NET_J1_13_GEN
14 NET_J1_14_GEN
TP40
TP41
TP42
TP43
CR16
NET_CR16_OUT
CR15-1
CR15-2
NET_CR15_OUT
CR14
NET_CR14_OUT
C1
CR7-2
CR7-1
A1t 34
CR5-1
CR5-2
JAt 20
NET_CR5_OUT
CR1-1
CR1-2
0.25V Skottky
NET_CR1_IN1
NET_CR1_IN2
TP6
R24
TP15
+BATT C4
C4
TP13
R30
TP28
+BATT C2
C2
NET_C2_PLUS
U3-1
U3-8
U3-2
U3-7
U3-3
U3-6
U3-4
U3-5
NET_PROG_P1
U3 ESDA25b1
GND
GND
GND
GND
GND
CR8-2
CR8-1
A1t 34
CR6-1
CR6-2
JAt 20
NET_CR6_OUT
F1
NET-C7-PLUS
+BATT C7
Supercap
C7
R27
R23
CZ1
zener diode?
Direction unknown
NET_U6_02
TP2
GND
GND
Voltage drop 0.6V for each diode
Sheet: /Input/
File: Input.kicad_sch
Title:
Size: A4
Date:
Rev:
KiCad E.D.A. kicad 7.0.2
Id: 3/4

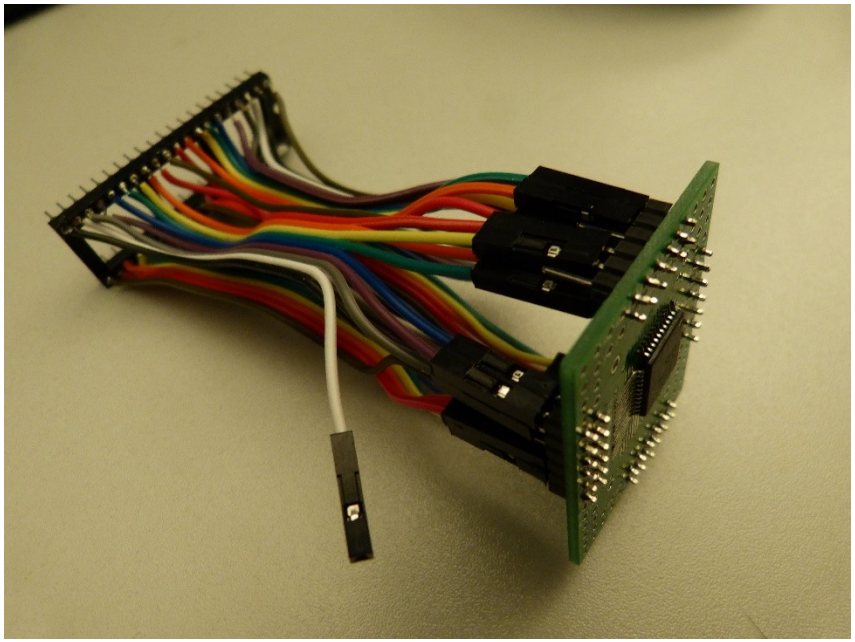

U1
P87C52
U2_VDD
VCC
VSS
GND
NET_U1_04
RST
/PSEN
ALE
/EA
NIC
XTAL2
XTAL1
TP73
R5
C5
C
TP141
TP140
TP34
TP86
TP85
P0.0
P0.1
P0.2
P0.3
P0.4
P0.5
P0.6
P0.7
P1.0
P1.1
P1.2
P1.3
P1.4
P1.5
P1.6
P1.7
P2.0
P2.1
P2.2
P2.3
P2.4
P2.5
P2.6
P2.7
P3.0
P3.1
P3.2
P3.3
P3.4
P3.5
P3.6
P3.7
NET_U1_37
NET_U1_36
NET_U1_35
NET_U1_34
NET_U1_33
NET_U1_32
NET_U1_31
NET_U1_30
NET_U1_40
NET_U1_41
NET_U1_42
NET_U1_43
NET_U1_44
NET_U1_01
NET_U1_02
NET_U1_03
NET_U1_18
NET_U1_19
NET_U1_20
NET_U1_21
NET_U1_22
NET_U1_23
NET_U1_24
NET_U1_25
NET_U1_05
NET_U1_07
NET_U1_08
NET_U1_09
NET_U1_10
NET_U1_11
NET_U1_12
NET_U1_13
TP77
TP76
TP1
TP146
TP63
TP33
TP138
P1
TP75
TP145
TP144
TP133
TP136
TP55
TP61
TP139
Quadrature in
Quadrature in
TP81
TP137
U14
R46
Q23
Q7
TP69
TP65
C18
C12
TP23
TP24
TP68
TP27
R32
R31
R7
R6
FB1
FB2
NET_SCL_LCD
NET_SDA_LCD
Q11
TP22
Q10
TP16
R12
CR12
TP21
Q9
TP25
Q8
TP30
VCC_EEPROM
U100
24LC01
SDA
SCL
WP
VCC
A0
A1
A2
NET_Q7_3
R29
R28
Q15
TP46
R26
TP31
TP48
R33
CR2
NET_J2_2
TP38
Mot
NET_U1_42
Q17
NET_U1_43
Q16
TP60
R3
TP29
Q3
+BATT C2
Testpoints_temp
File: untitled.kicad_sch
Input
File: Input.kicad_sch
LCD_Driver
File: LCD.kicad_sch
Sheet: /
File: XO_HWRE.kicad_sch
Title:
Size: A4
Date:
Rev:
KiCad E.D.A. kicad 7.0.2
Id: 1/4

8051

riscure

- Xgcu TI866II Programmer with Xgpro
  - Changed to Minipro (CLI)
- Locked & fused & encrypted

- Acquired open samples
  - Ebay, not cheap
  - Pre-programmed ☹



Xgpro v10.80

File(F) Select IC(S) Project(P) Device(D) Tools(V) Help(H) Language(L)

LOAD SAVE AUTO CHECK BLANK VERIFY READ ADD RAM Erase PROG. ABOUT CALCU. TV

Select IC

P87C58U

IC Information(No Project opened)

ChipType: MCU/MPU ChkSum: 0x0054 DF34

IC Size: 0x8000 Bytes (32768 Bytes) + 0x40 Bytes

XGecu® Pro

Set Interface

ZIF socket ICSP port ICSP_VCC Enable

Vcc current Imax: Default 8 Bits 16 Bits

Upgrade is available

Save Log Clear

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
0000-0000:	02	00	90	32	FF	FF	FF	FF	FF	FF	FF	30	07	10	D2	0D	...2.......0....
0000-0010:	32	FF	FF	30	07	02	D2	0E	32	FF	FF	02	00	90	02	03	2..0....2.......
0000-0020:	CD	FF	FF	32	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	...2............
0000-0030:	44	46	4D	30	36	2D	31	20	20	20	20	20	20	20	20	20	DFM06-1
0000-0040:	52	45	4C	2D	41	2D	56	30	2D	43	31	2D	45	31	20	20	REL-A-V0-C1-E1
0000-0050:	56	35	2E	32	30	2E	30	32	20	20	20	20	20	20	20	20	V5.20.02
0000-0060:	32	30	30	39	2D	31	32	2D	31	36	20	20	20	20	20	20	2009-12-16
0000-0070:	4D	61	72	6B	75	73	20	48	61	69	73	74	20	20	20	20	Markus Haist
0000-0080:	4D	48	69	6E	74	65	72	66	61	63	65	20	20	00	00	00	MHinterface ...
0000-0090:	90	01	FE	12	08	A4	FC	F5	49	05	82	12	08	A4	F5	4A	........I......J
0000-00A0:	5C	B4	FF	04	C2	49	C2	4A	75	81	5F	12	0A	9B	12	08	\....I.Ju._.....
0000-00B0:	5A	D2	B4	75	88	00	75	89	51	75	98	00	75	B8	00	D2	Z..u..u.Qu..u...
0000-00C0:	88	D2	8A	C2	A8	C2	AA	C2	A9	C2	AB	D2	AF	12	0A	A2	....
0000-00D0:	75	81	5F	12	0B	7E	12	04	E9	75	83	00	75	82	04	12	u._..~...u..u...
0000-00E0:	08	A4	A2	E7	92	09	D2	B7	30	B7	03	02	06	01	02	0D	........0.......
0000-00F0:	40	A8	E2	00	00	00	00	00	00	65	54	00	01	00	01	00	@........eT.....
0000-0100:	00	38	4B	00	02	00	02	00	00	1E	66	00	04	00	03	00	.8K.......f.....
0000-0110:	00	0F	33	00	08	00	04	00	00	07	99	00	10	00	05	00	..3.............
0000-0120:	00	03	CC	00	20	00	06	00	00	01	E6	00	40	00	07	00	....@...
0000-0130:	00	00	F3	00	80	00	08	00	00	00	00	01	00	00	09	00	....
0000-0140:	00	09	CC	01	00	00	09	00	00	04	E6	02	00	00	0A	00	....
0000-0150:	00	02	73	04	00	00	0B	00	00	01	39	08	00	00	0C	00	..s.......9.....
0000-0160:	00	00	A1	10	00	00	0D	00	00	00	00	00	62	00	0F	00	............b...
0000-0170:	00	C2	07	C2	06	20	09	03	02	03	07	85	81	41	C2	AA	....A..
0000-0180:	D2	A8	D2	A9	75	3A	00	74	01	75	8C	00	75	8A	00	D2	....u:.t.u..u...
0000-0190:	8C	42	87	75	8A	00	75	8C	00	42	87	C2	8C	85	8C	43	.B.u..u..B.....C

```
**************************************************
 1 Programmer Connected.
**************************************************
  Device 1: TL866II-Plus Ver: 04.02.124
       USB SPEED MODE: FS 12MHZ
**************************************************

P87C58U
  Memory Size : 0x00008000
```

FLASH Encryp.TB Config Device.Info

Options

- [x] Pin Detect
- [ ] Check ID
- [ ] Erase before
- [x] Verify after
- [ ] Auto SN_NUM
- [ ] Skip Blank
- Addr.Range: (•) ALL ( ) Sect
- [ ] Blank Check
- 0x 00000000 -> 00007FFF

IC Config Informaton

Lock Byte: 0x00

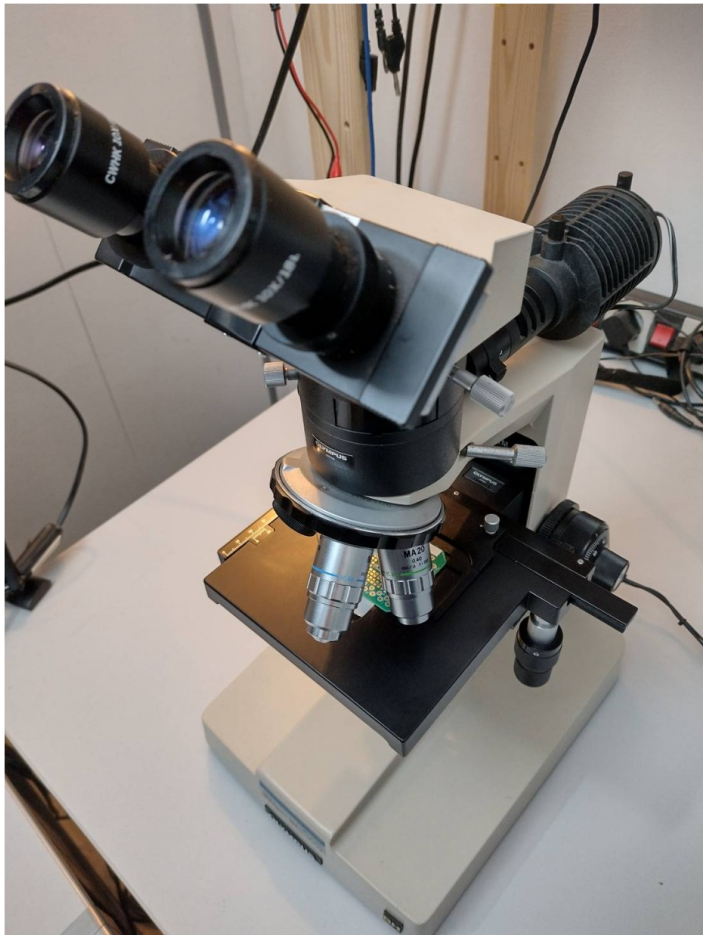
Ready

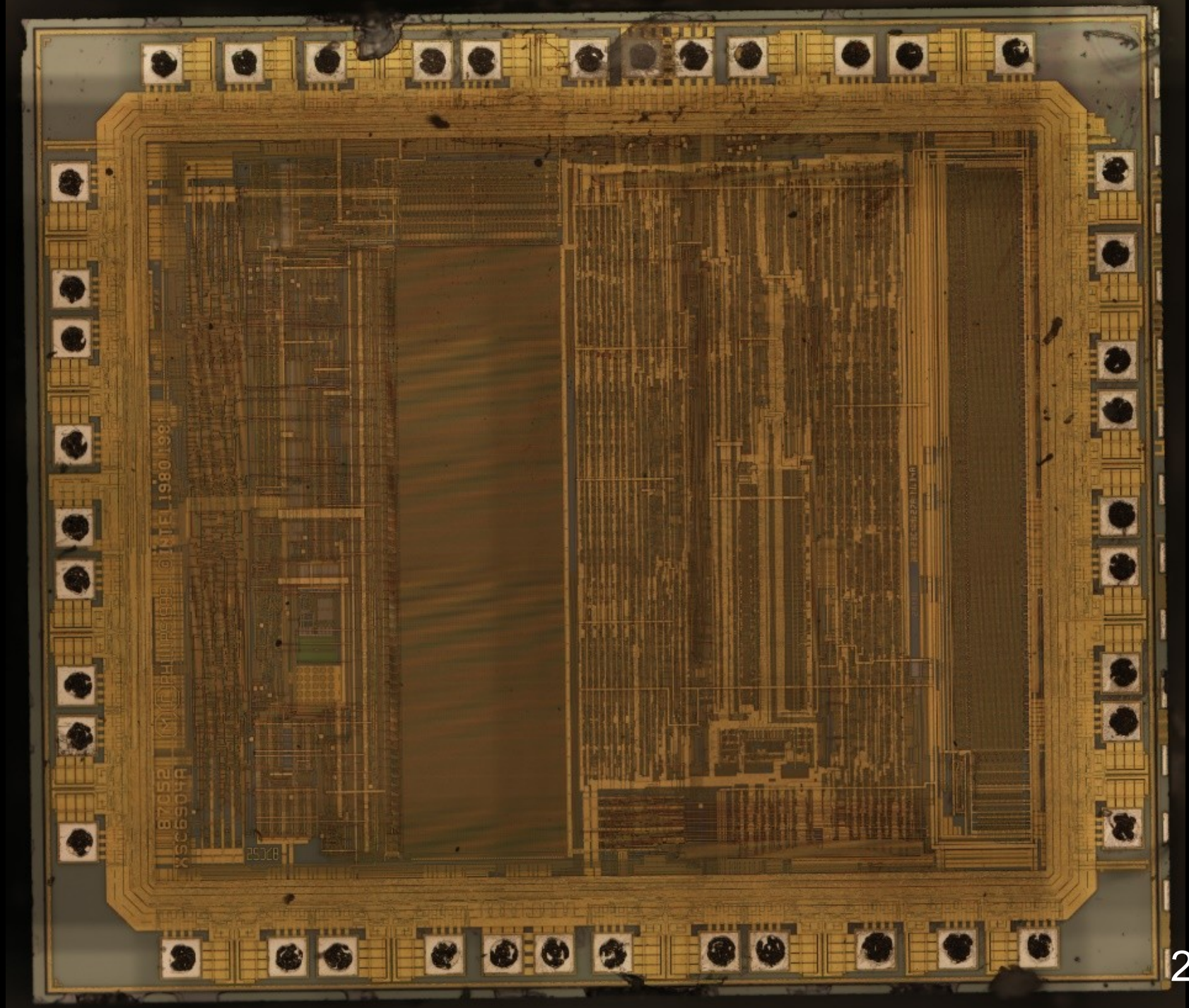
Default Programmer(1): TL866II-Plus

0000 0000

Chip reverse engineering

- Decap many chips
  - Heat & twist
- Photographing
  - Metallurgical microscope
  - Stitching – 208MP
- Ideas for the future
  - Micro probing
  - Visiting friends with a SEM
  - International collaboration

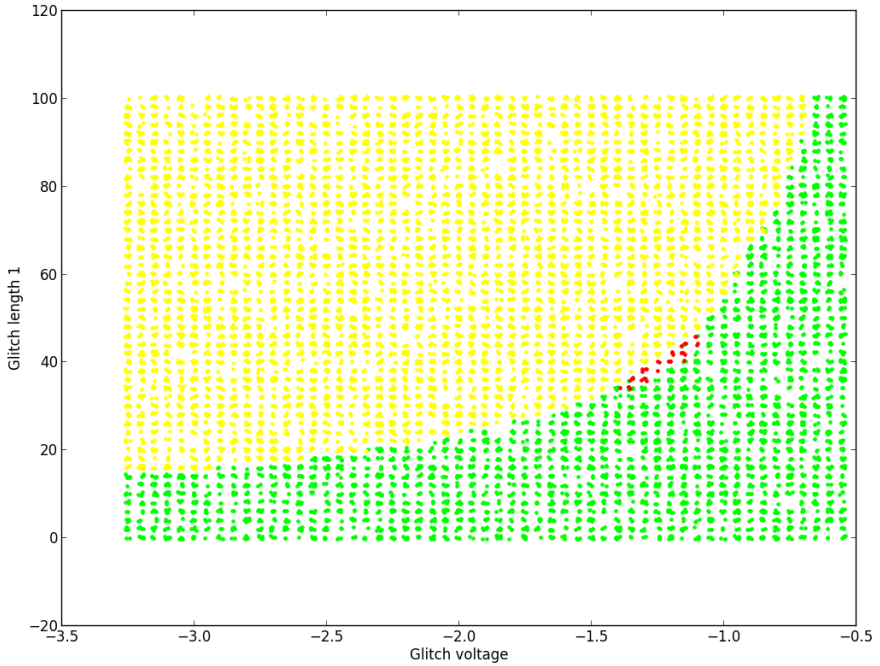



87052
XSC6504A
©INTEL 1980 '98

1980

Fault injection

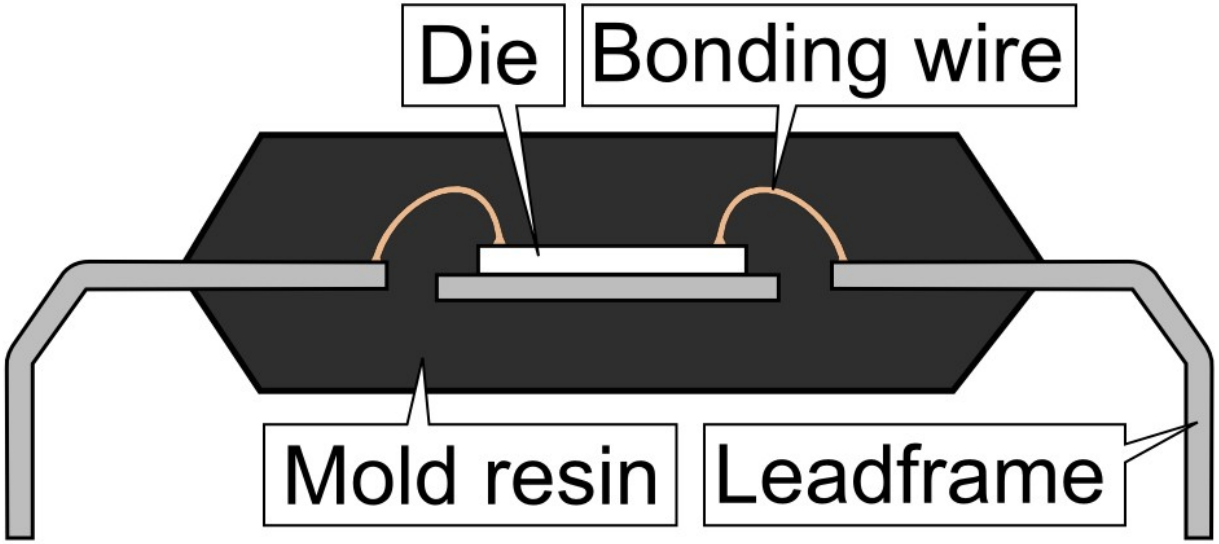
- (Non) invasive Hardware attack
  - Relatively straightforward process
  - Basic setup for <€1000
  - Difficult to do right
- Methods
  - Voltage
  - Timing
  - Clock
  - Electromagnetic
  - Lasers

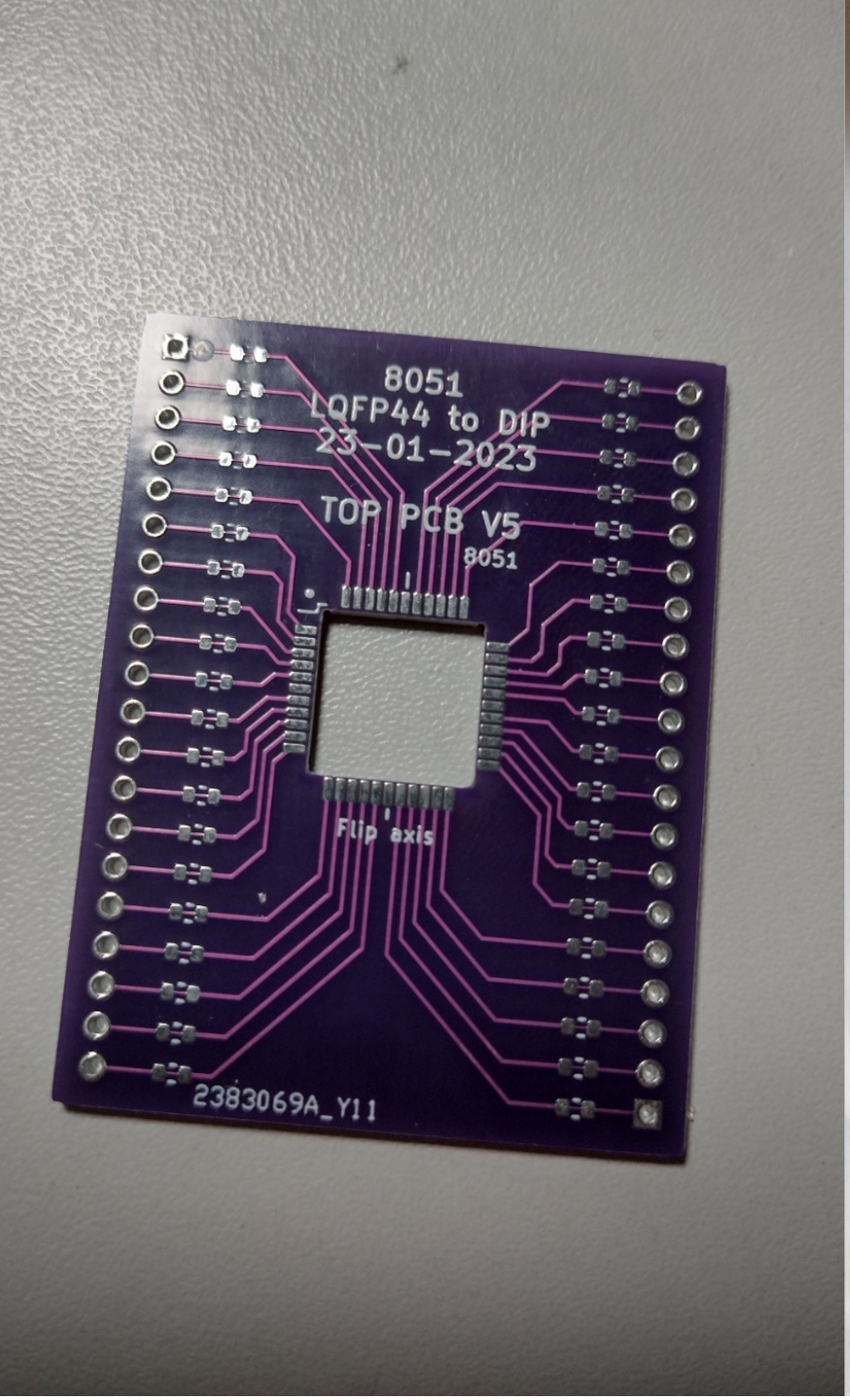


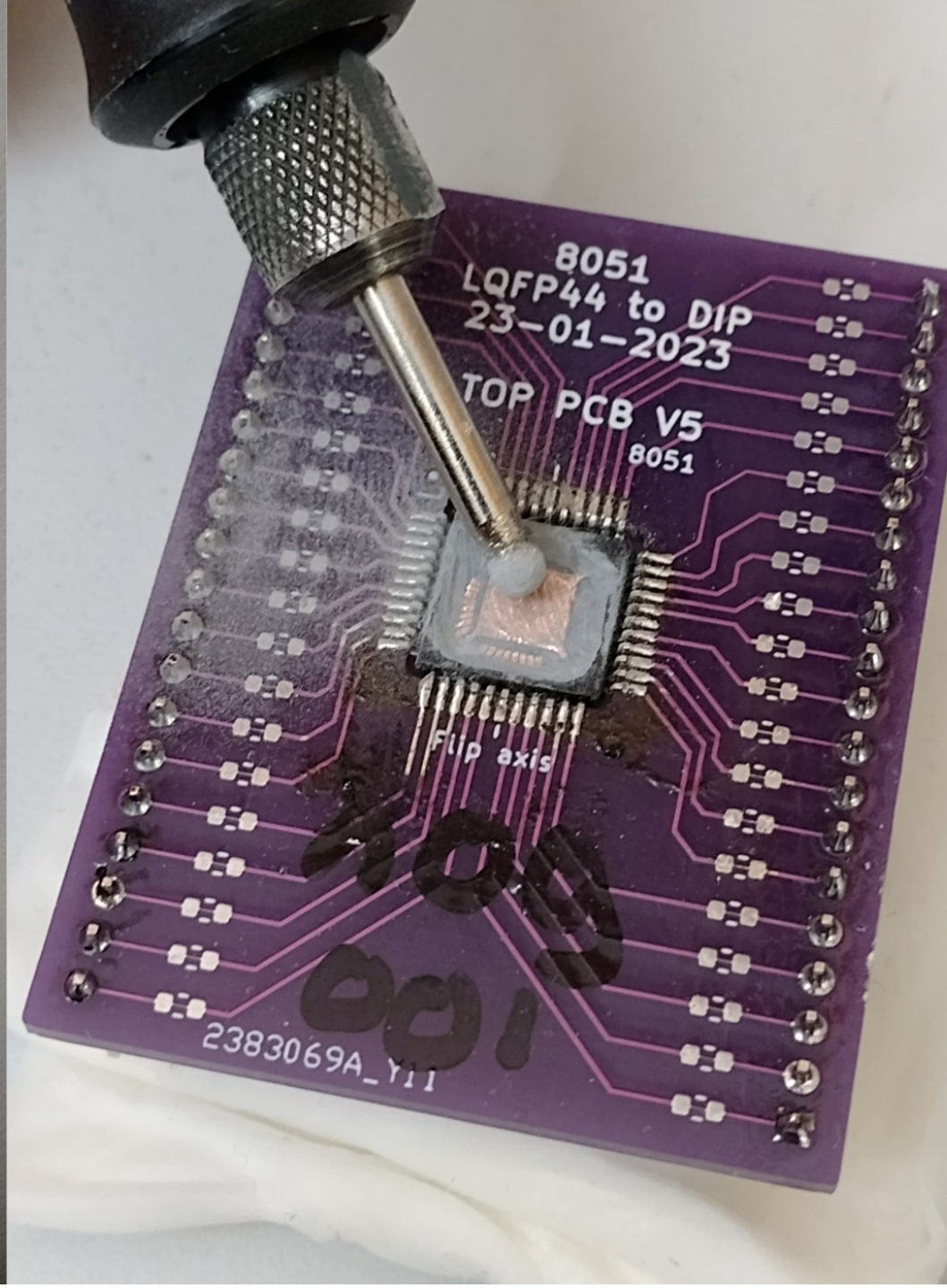
Fault injection

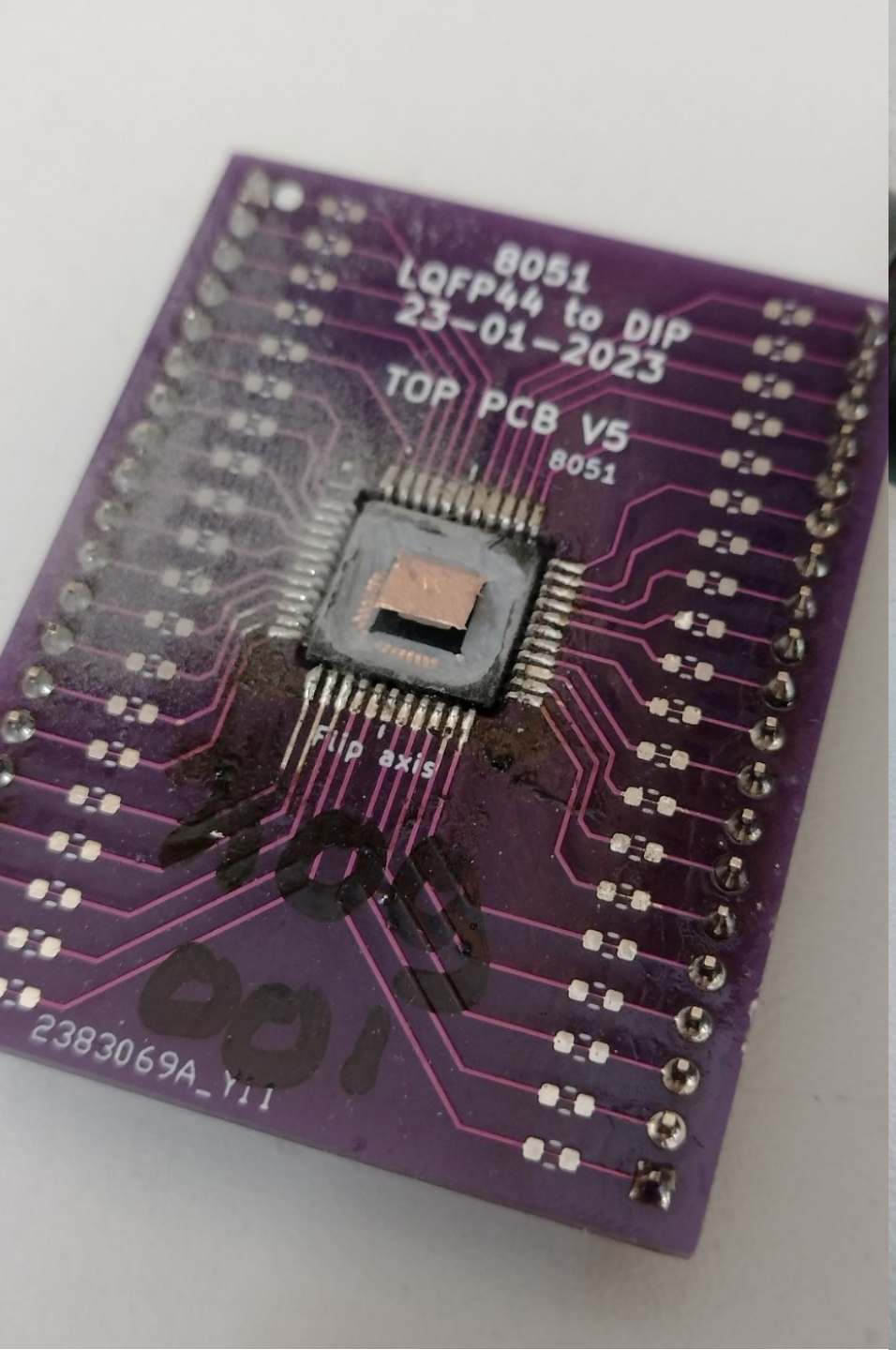
riscure

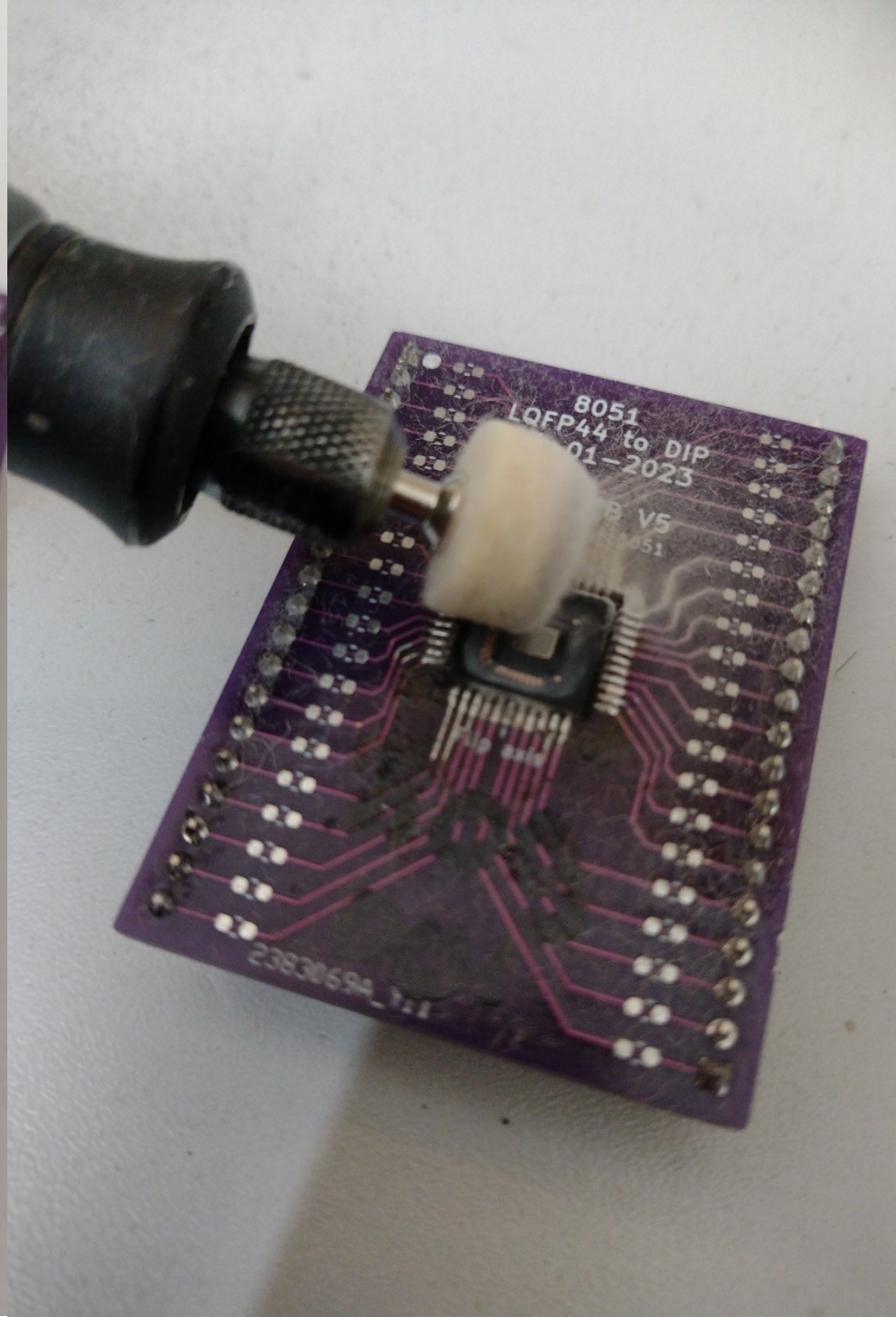
- Sample preperation for Laser FI
  - Chip side
    - Dangergous chemicals
  - Back side
    - Easy mechanical process

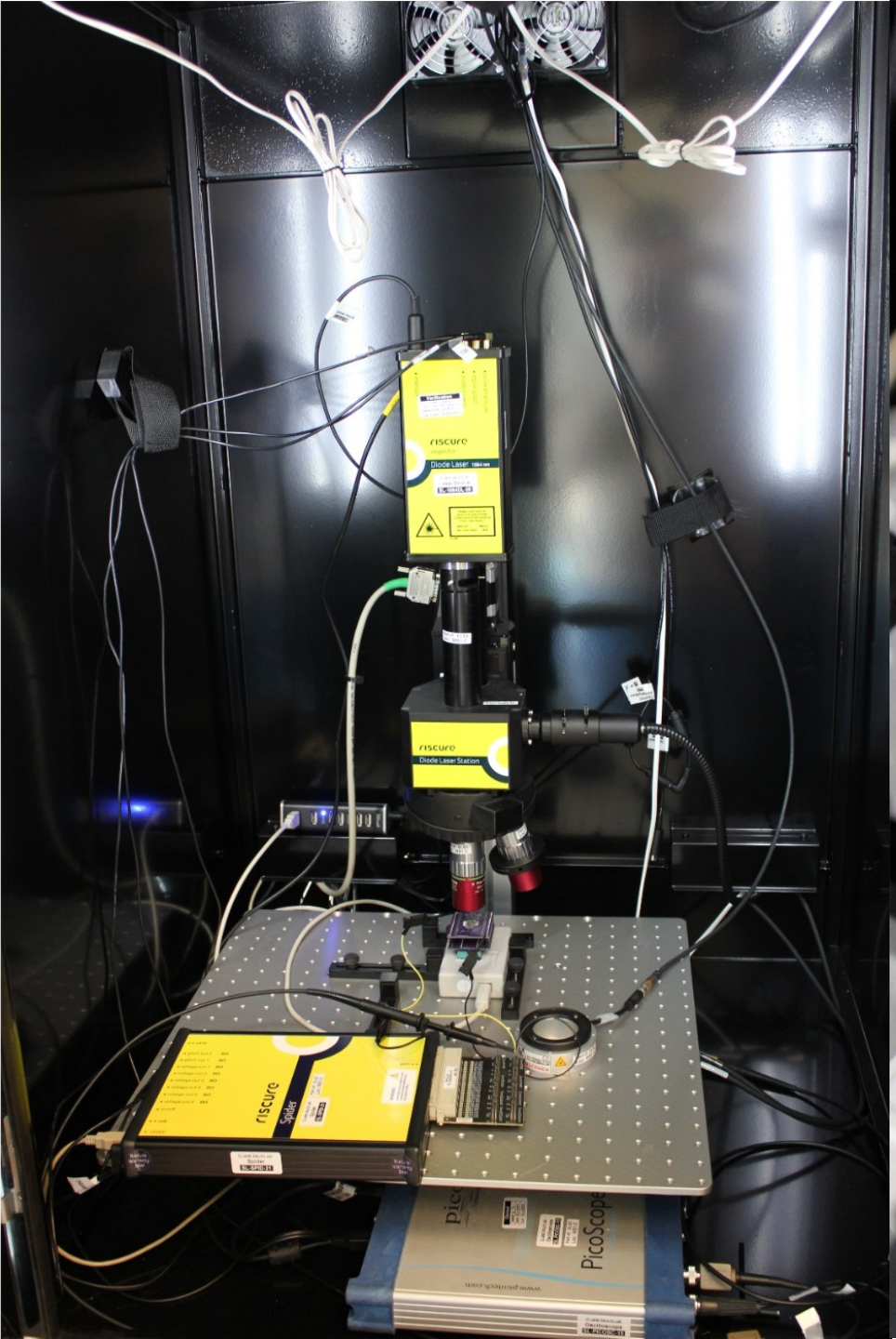


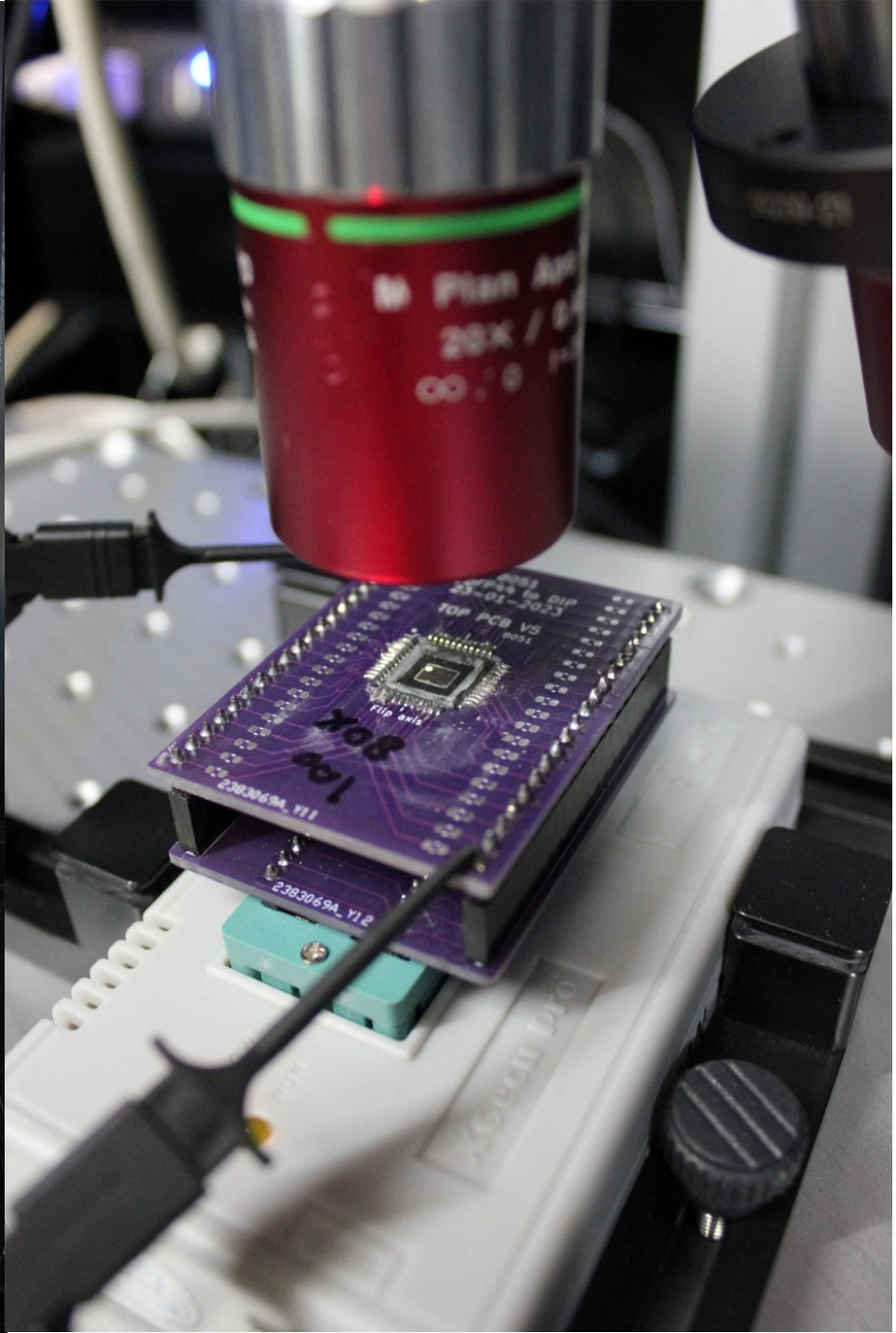

8051
LQFP44 to DIP
23-01-2023
TOP PCB V5
8051
Flip axis
2383069A_Y11

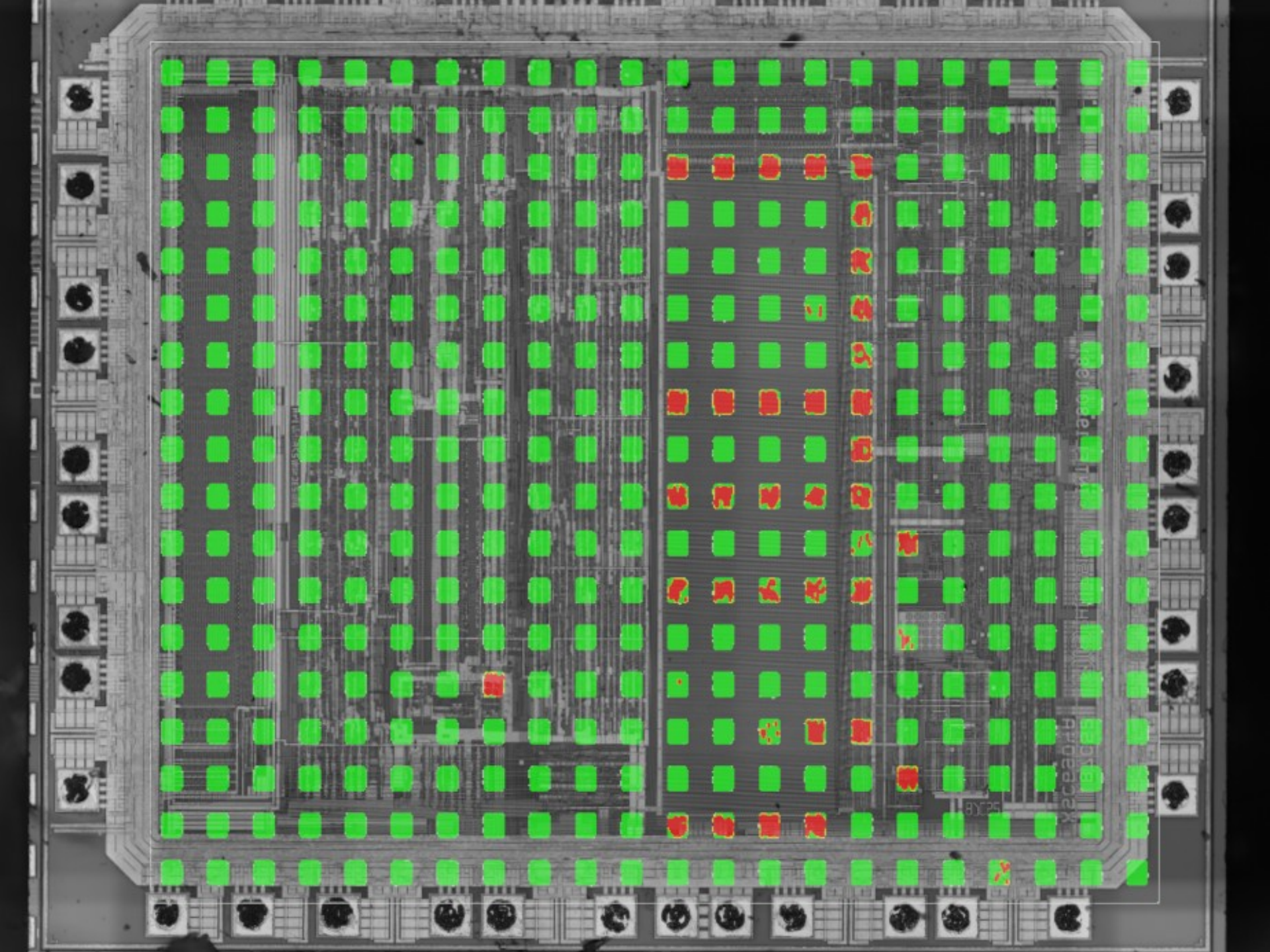

8051
LQFP44 to DIP
23-01-2023
TOP PCB V5
8051
Flip axis
2383069A_Y11

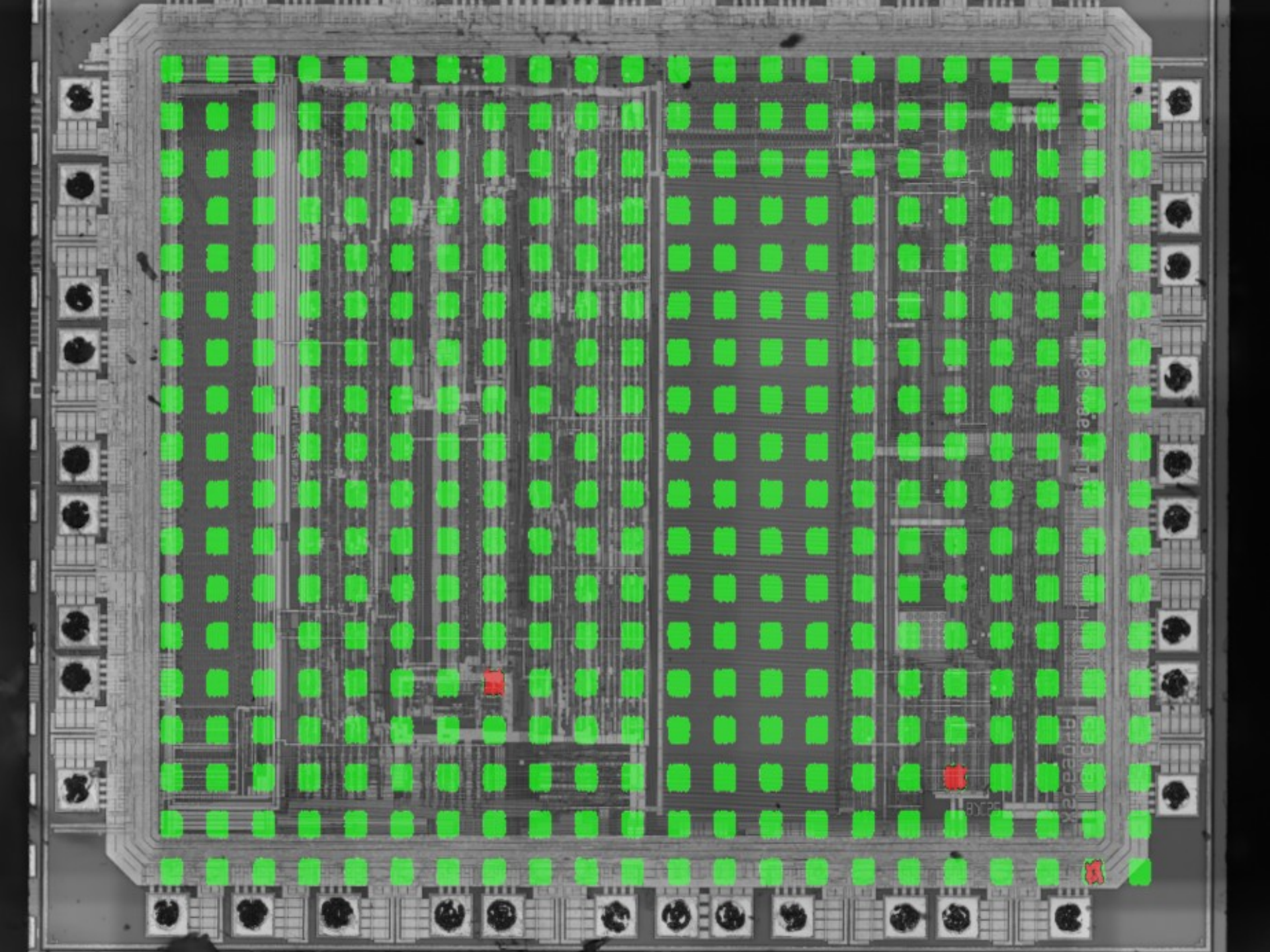

8051
LQFP44 to DIP
23-01-2023
TOP PCB V5
8051
Flip axis
2383069A_V11


8051
LQFP44 to DIP


riscure
Diode Laser
riscure
Diode Laser Station
riscure
Spider
PicoScope


TOP PCB V5
Flip axis
2383069A_V11
2383069A_V12



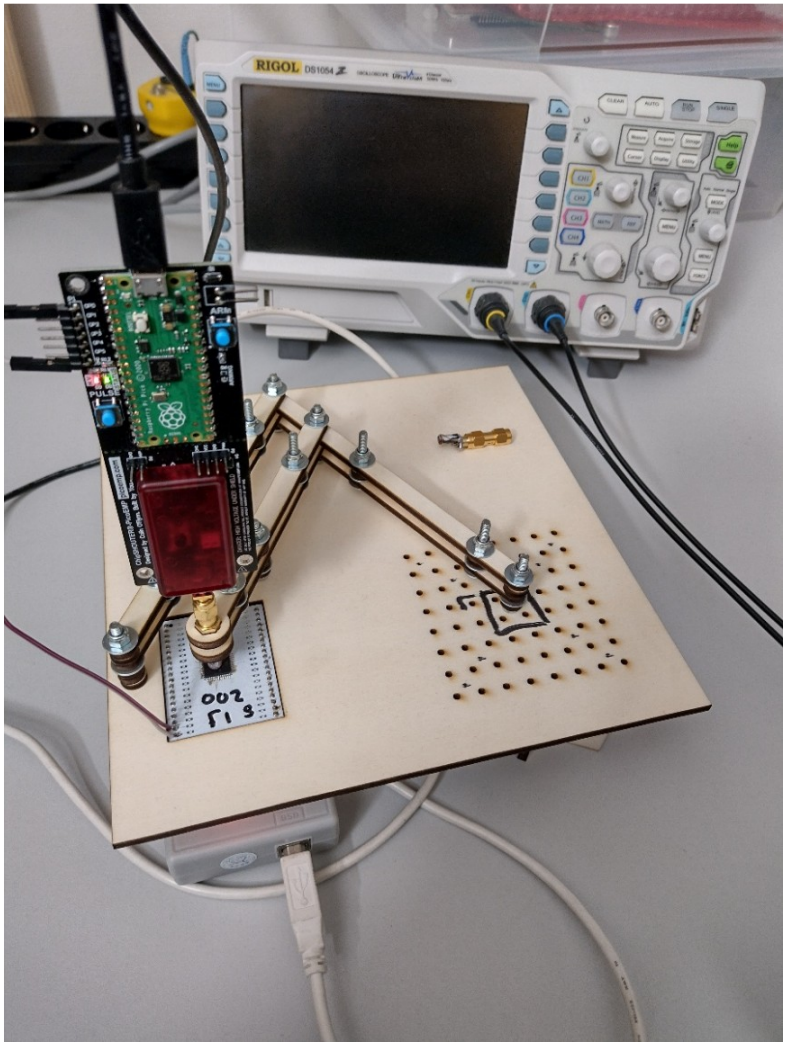


Laser = Success

- X07
  - Copyright 1990,91,92 Dan L. Thompson Mas-Hamilton Group
- X08
  - Copyright 1999 Mas-Hamilton Group
- X09
  - Copyright 2002 Kaba-Mas Dan Thompson

Fault injection

- PicoEMP
  - Colin O'Flynn (NewEA)
  - Opensource
  - € 100 in parts
  - Slightly underpowered
- Human XYZ
  - Pantograph

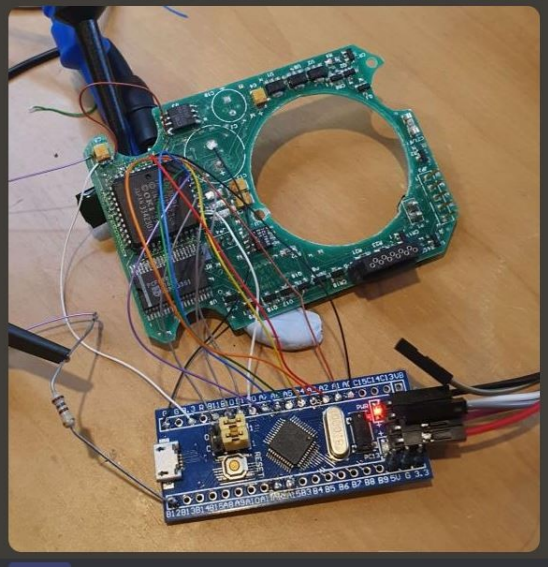


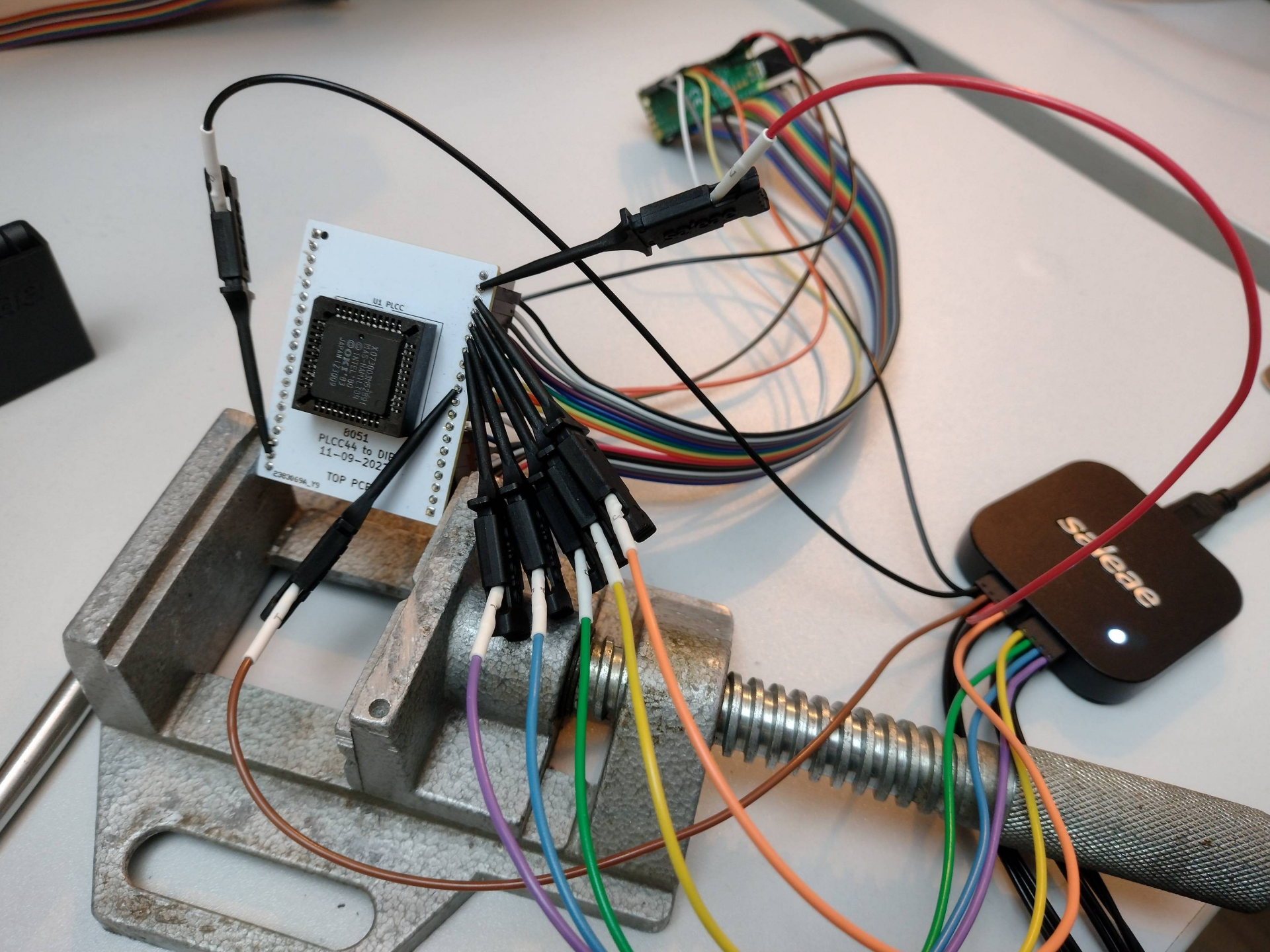
Try a more ‘Abrasive’ method

@Jan-Willem @abrasive Congrats on the work. I'd like to compare notes some time about the X0 memory dump. I've done something similar, but it was serious effort involving lasers...

abrasive Yesterday at 11:56 PM

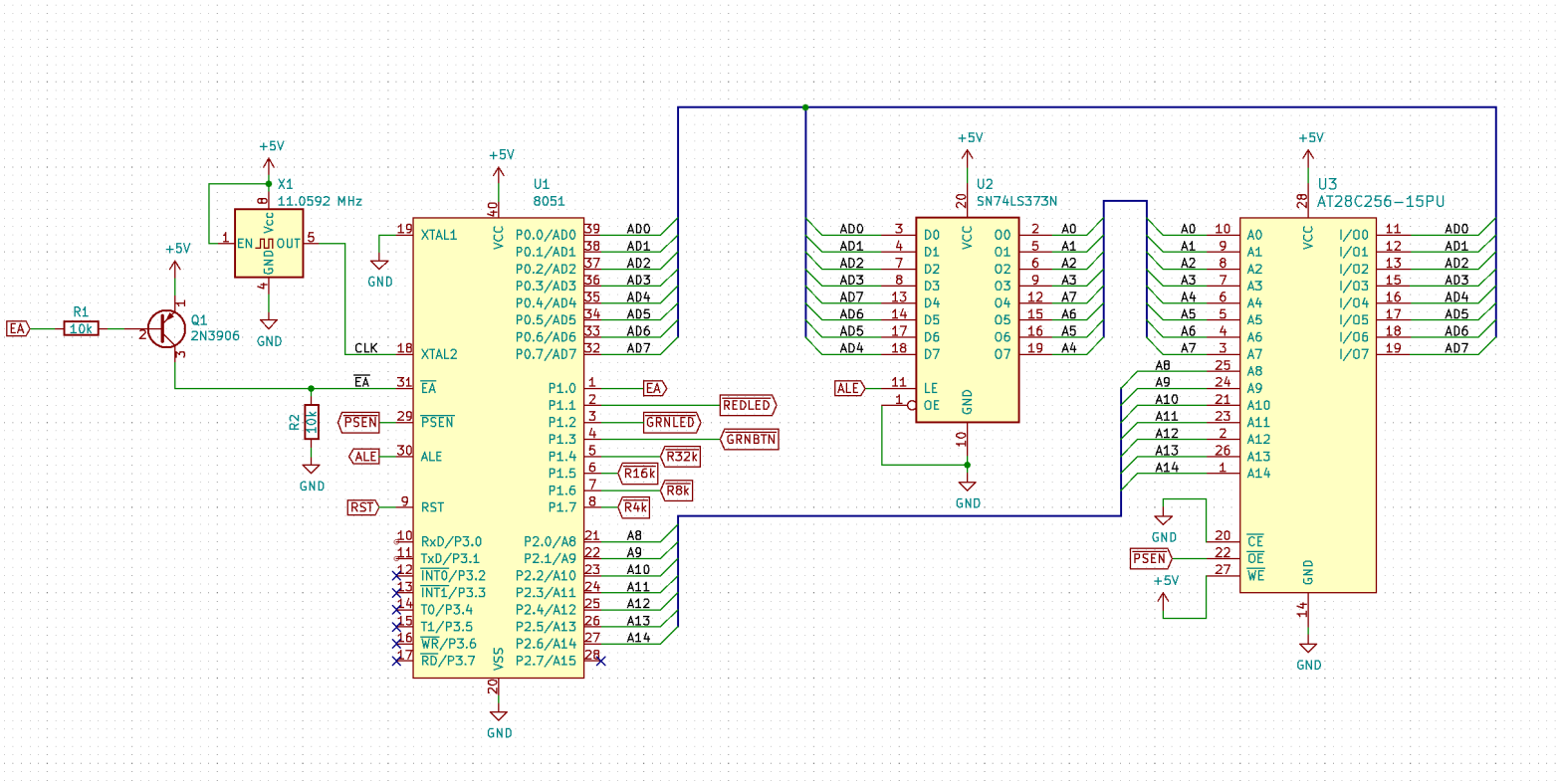
damn son, I didn't even desolder the target in the end




U1 PLCC
8051
PLCC44 to DIP
TOP PCB

‘Abrasive’ method

- 8051dumper
  - Mark J. Blair
  - https://gitlab.com/NF6X_Retrocomputing/8051dumper



riscure

Ketchup

Previous work

Inspiration

July 5, 2019

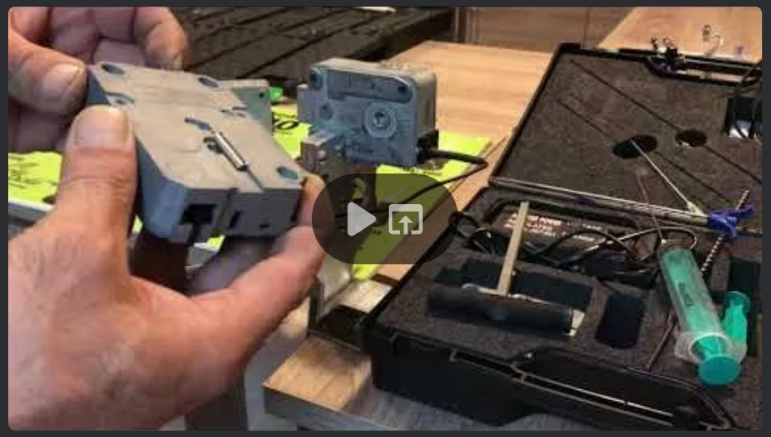
NKT 07/05/2019 2:12 PM

https://youtu.be/aWToH5C4JKY

YouTube

TURBODECODER LOCKSMITH PICK TOOLS FACTORY

Electronic safe locks opening demo with E Lock Shock kit !!



July 6, 2019

Jan-Willem Toool NL 07/06/2019 10:03 AM

@NKT

As an electrical engineer I'm quite confused.
The liquid shorts something, still it opens the lock.

Electronic safe locks opening demo with E Lock Shock kit !!

Turbo Decoder by LuckyLocks
9.72K subscribers

Subscribe

289 | Share | Download | Clip | Save

41K views 4 years ago
Innovative method to bypass the codes of the electronic safe locks.
The tool is also usefull when the lock is dead or when the owner forgot the code.
On our web site www.turbodecoder.com you can see the full list and specification of tested and opened locks. ...more

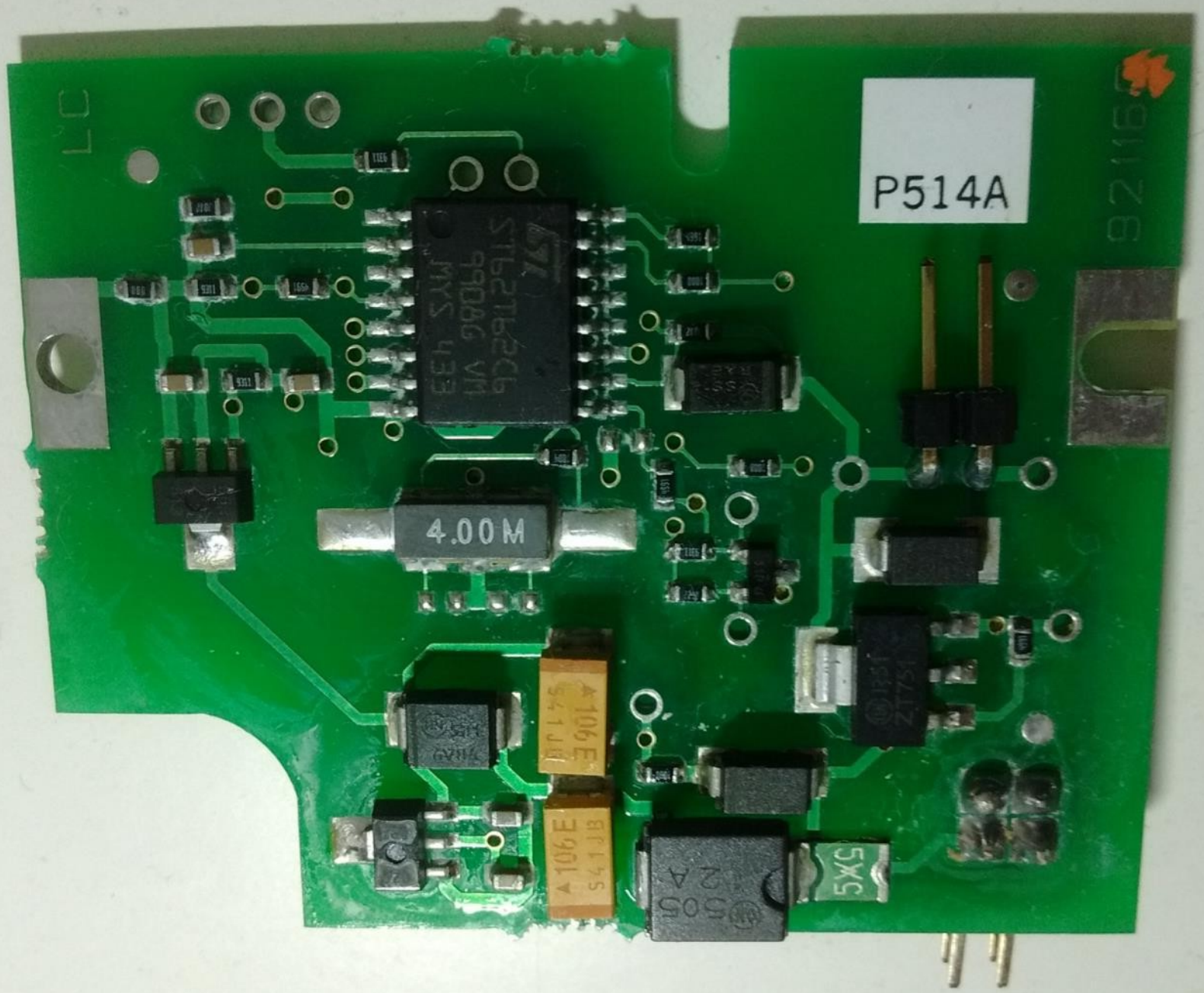
Turbodecoder

- Lock genius & Creators of advanced lock opening tools
  - E-LOCK SHOCK kit
  - €600. (refills at €50 a lock)
  - https://turbodecoder.com/product/e-lock-shock/

Ketchup opens locks

riscure

- Hypothesis:
  - The motor and power contacts are very close together.
  - The liquid is quite high resistance. (100 ohm/cm).
- Nigel added:
  - It seems no-one knows why it works, it just does.
  - Most people use ketchup, which is thick enough not to run away, and conductive enough to work.
- To do:
  - Pick up a bottle of ketchup and measure the conductivity.
  - Get an electronic lock and measure how it's wired.

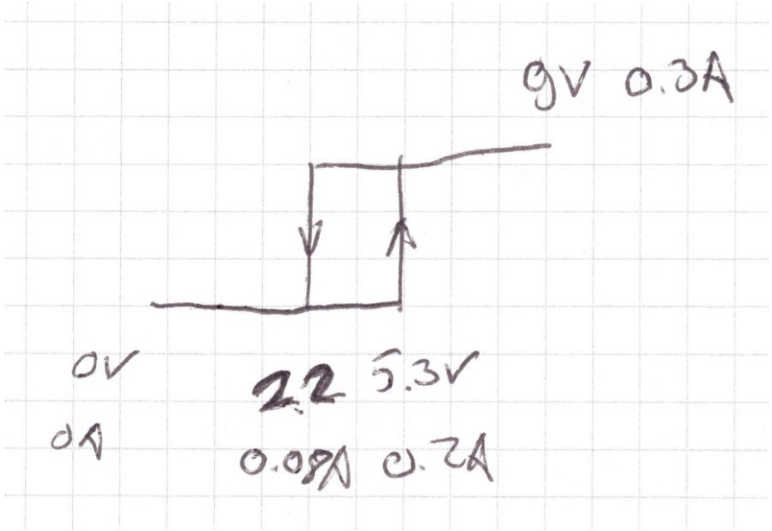

P514A
4.00M

Reverse engineering

riscure

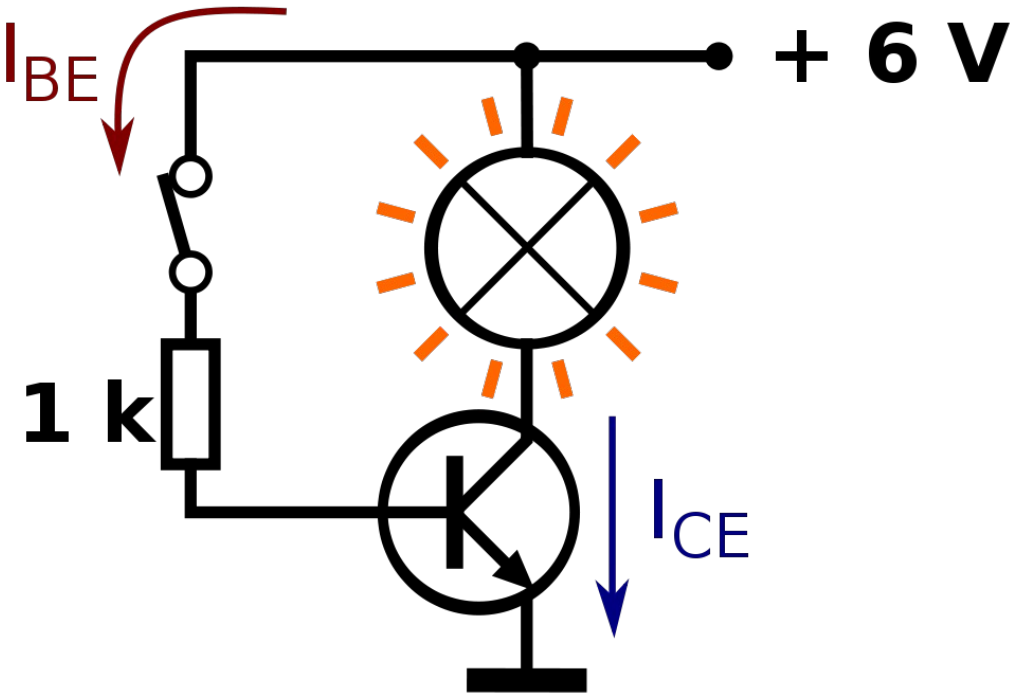
- Circuit board:
  - The microcontroller is a ST62T62C6
  - (OTP, Cheap, obsolete)
  - linear regulator 3.3V
  - 2222N NPN
  - ZT751 PNP

- Solonoid
  - N001 DET 0503A 10E04
  - Measurements:
  - Active: 5.3V, 0.2A
  - R = U/I = 26.5Ω
  - Non polarized

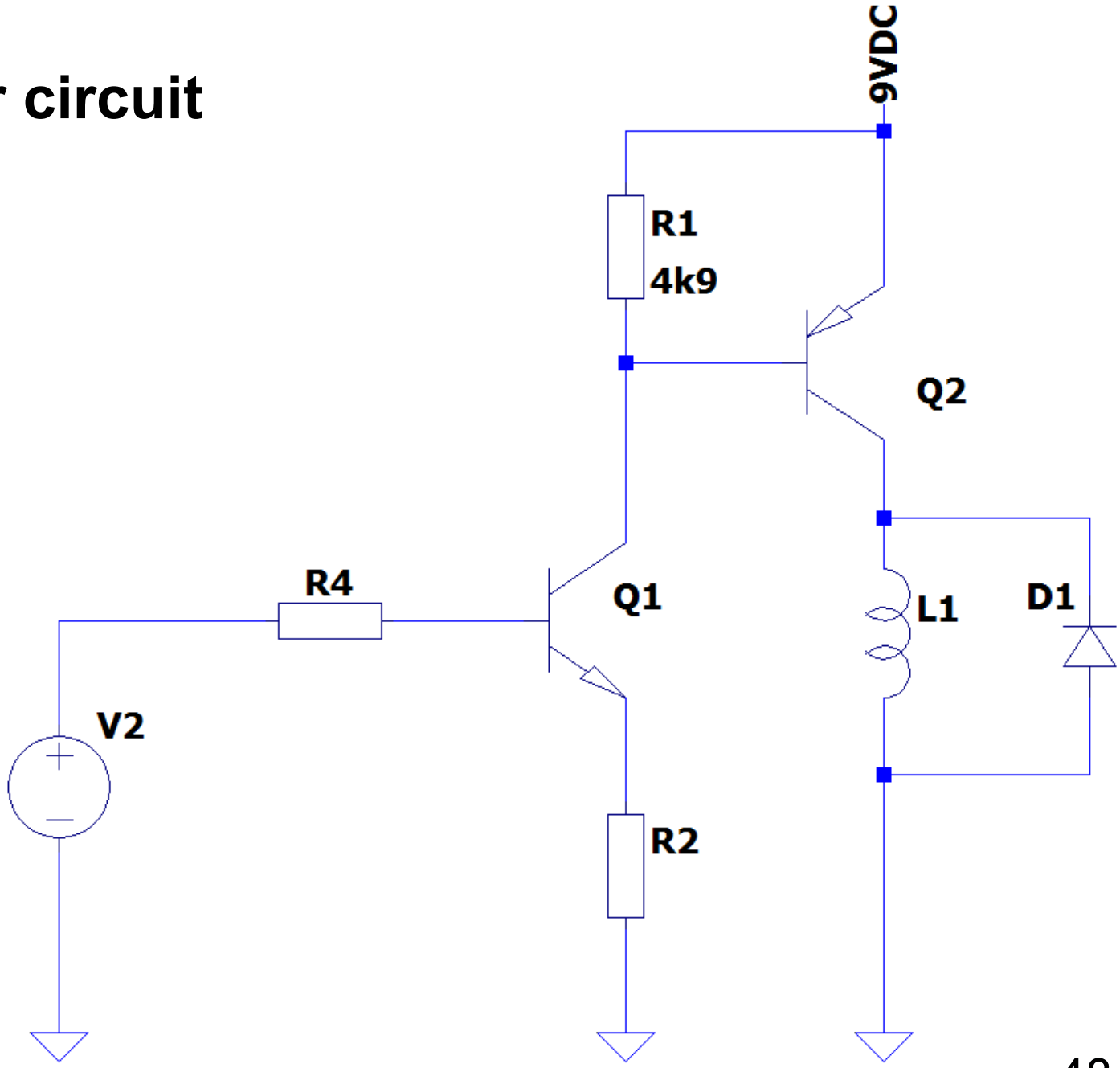


Transistor circuit

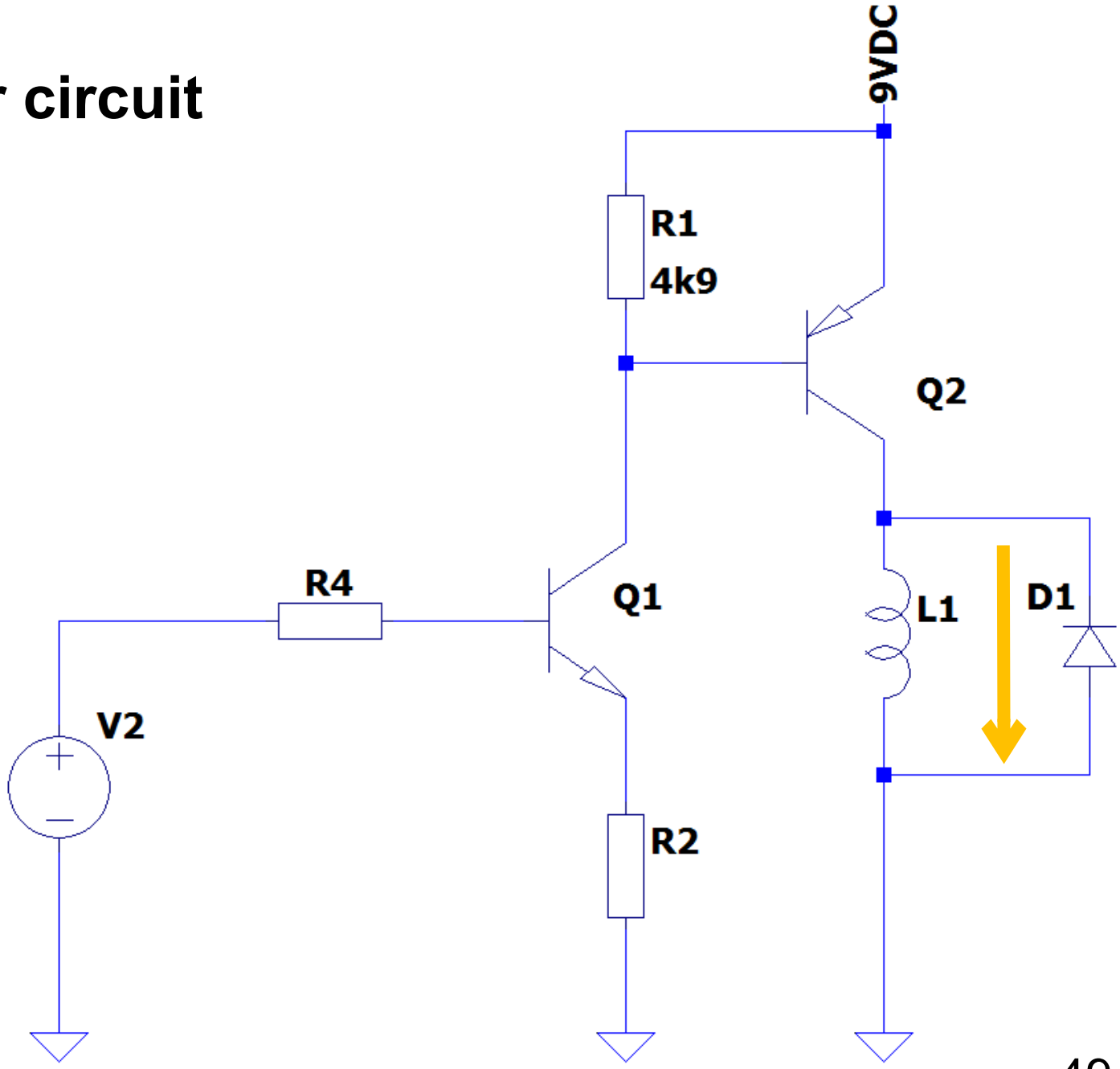
- Transistors = amplifiers
- Small current transistor -> High amplification (>100)
- Large current transistor -> Small amplification (<100)



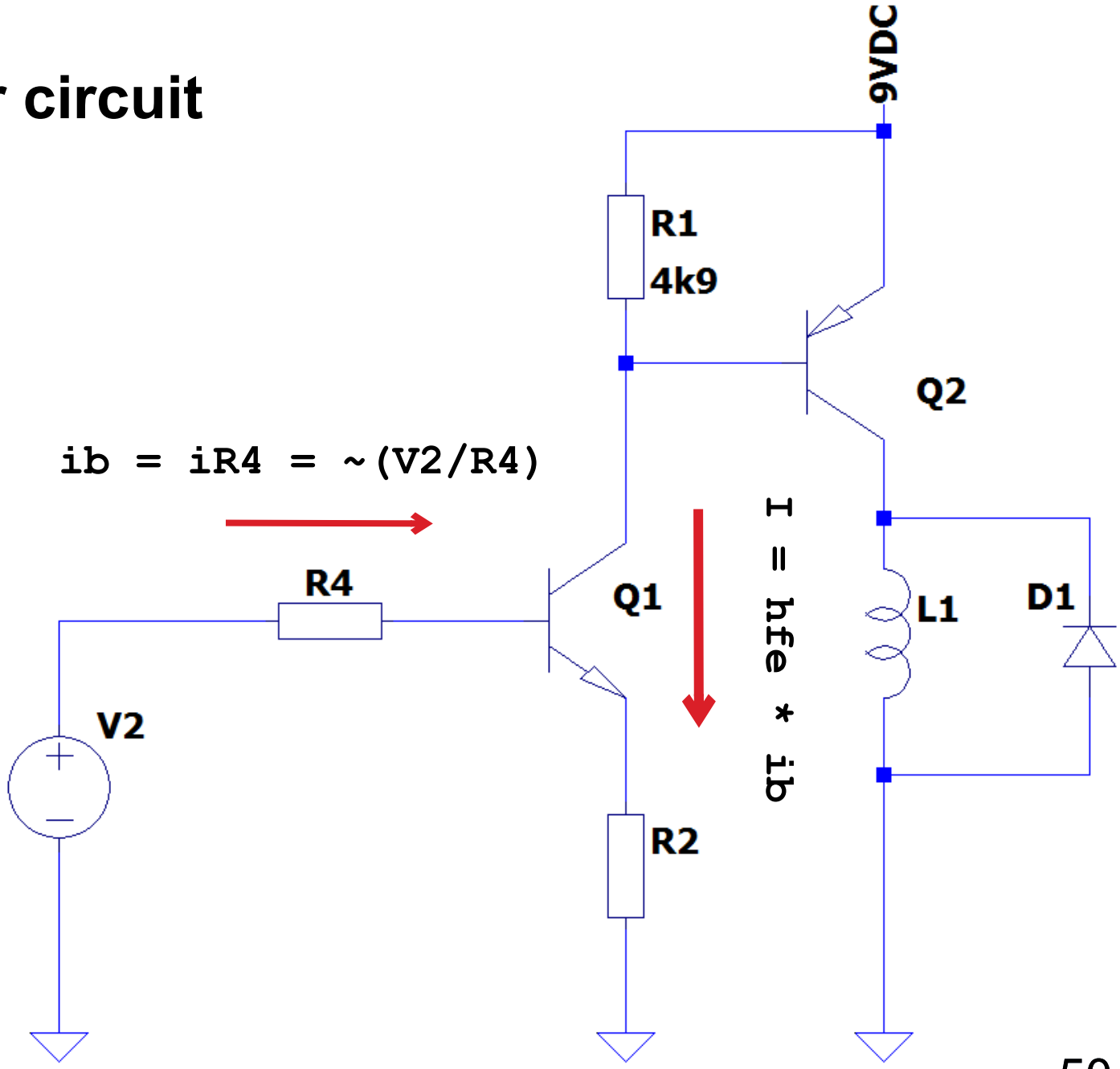
Transistor circuit



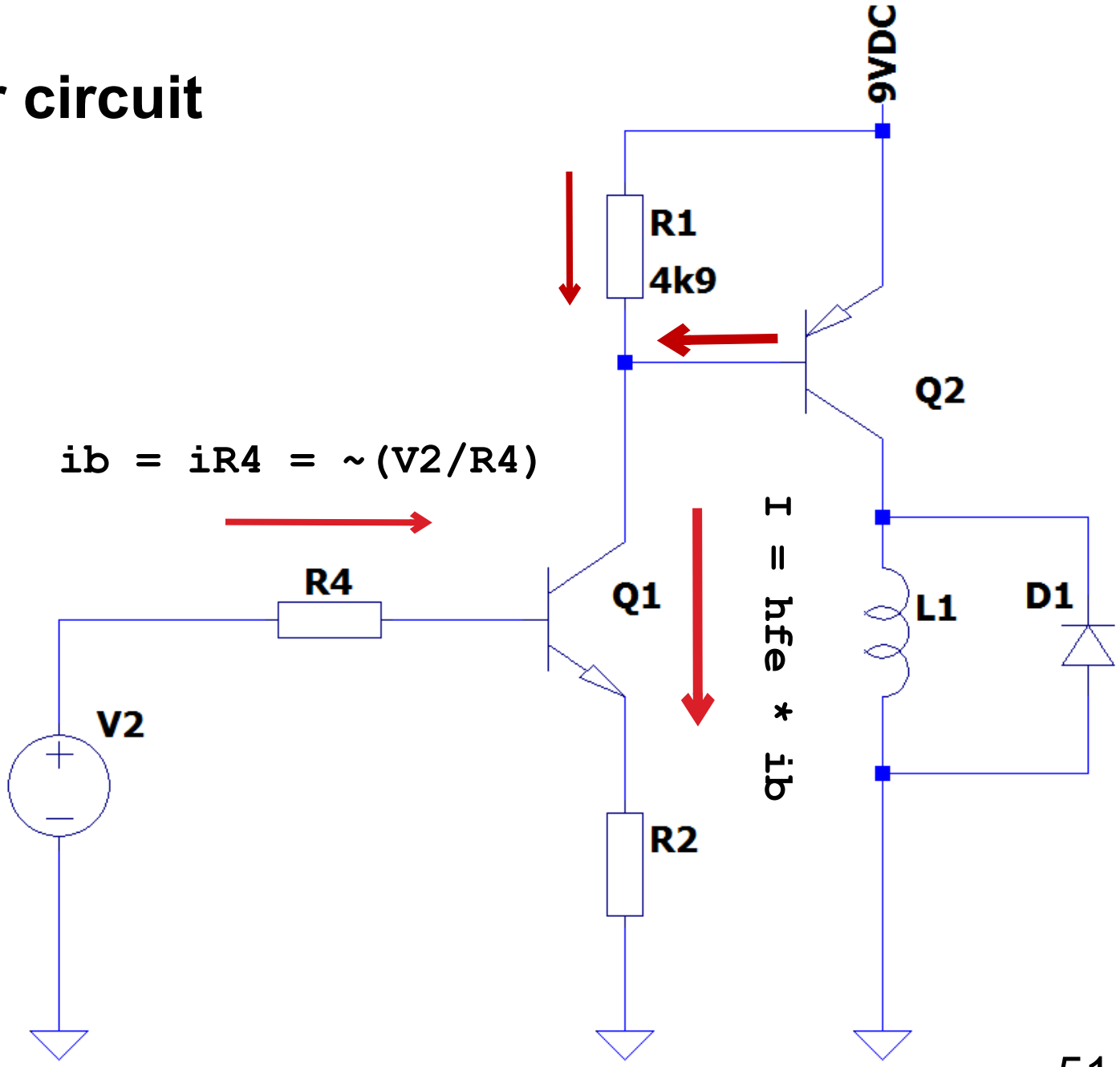
Transistor circuit



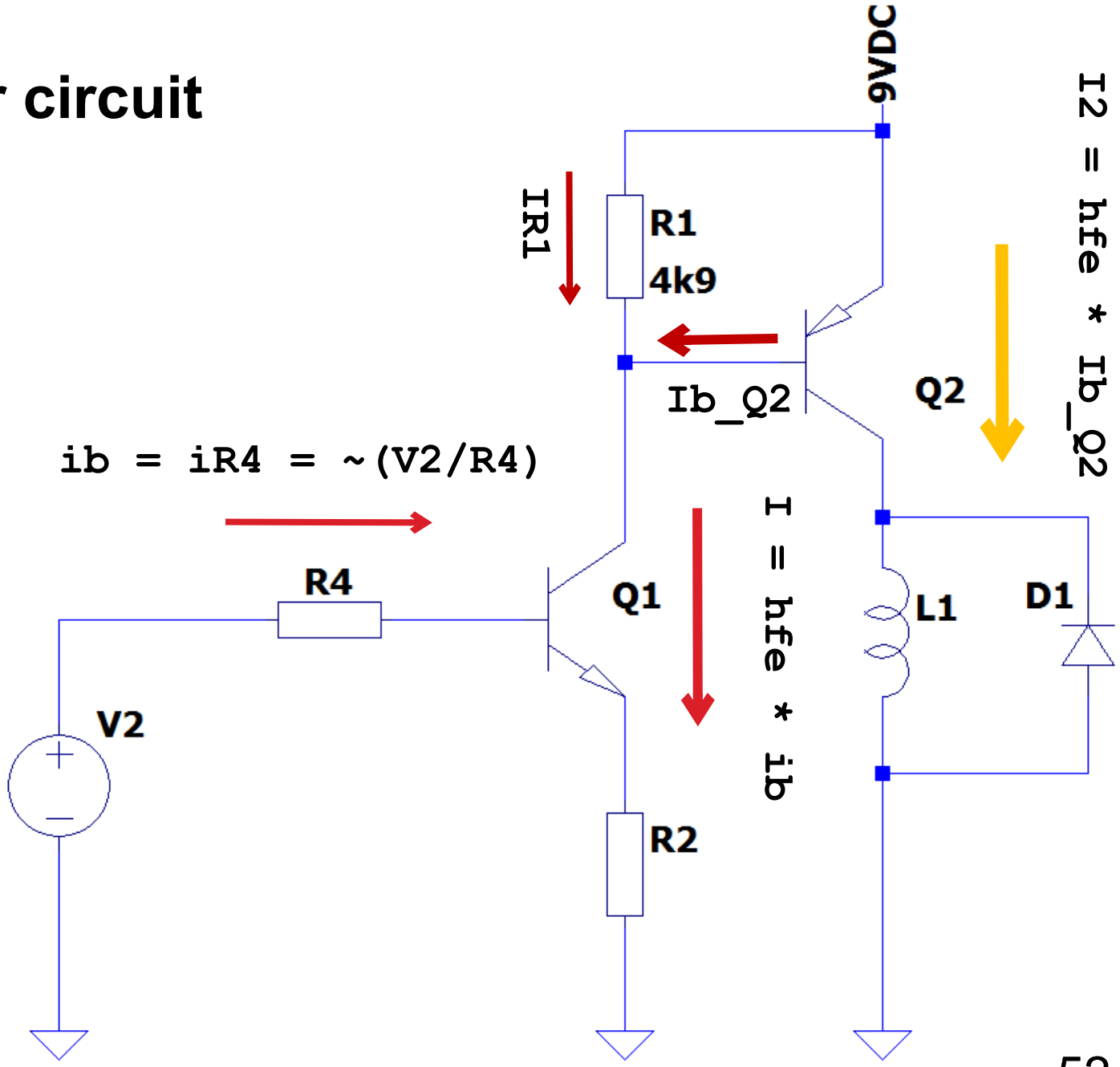
Transistor circuit



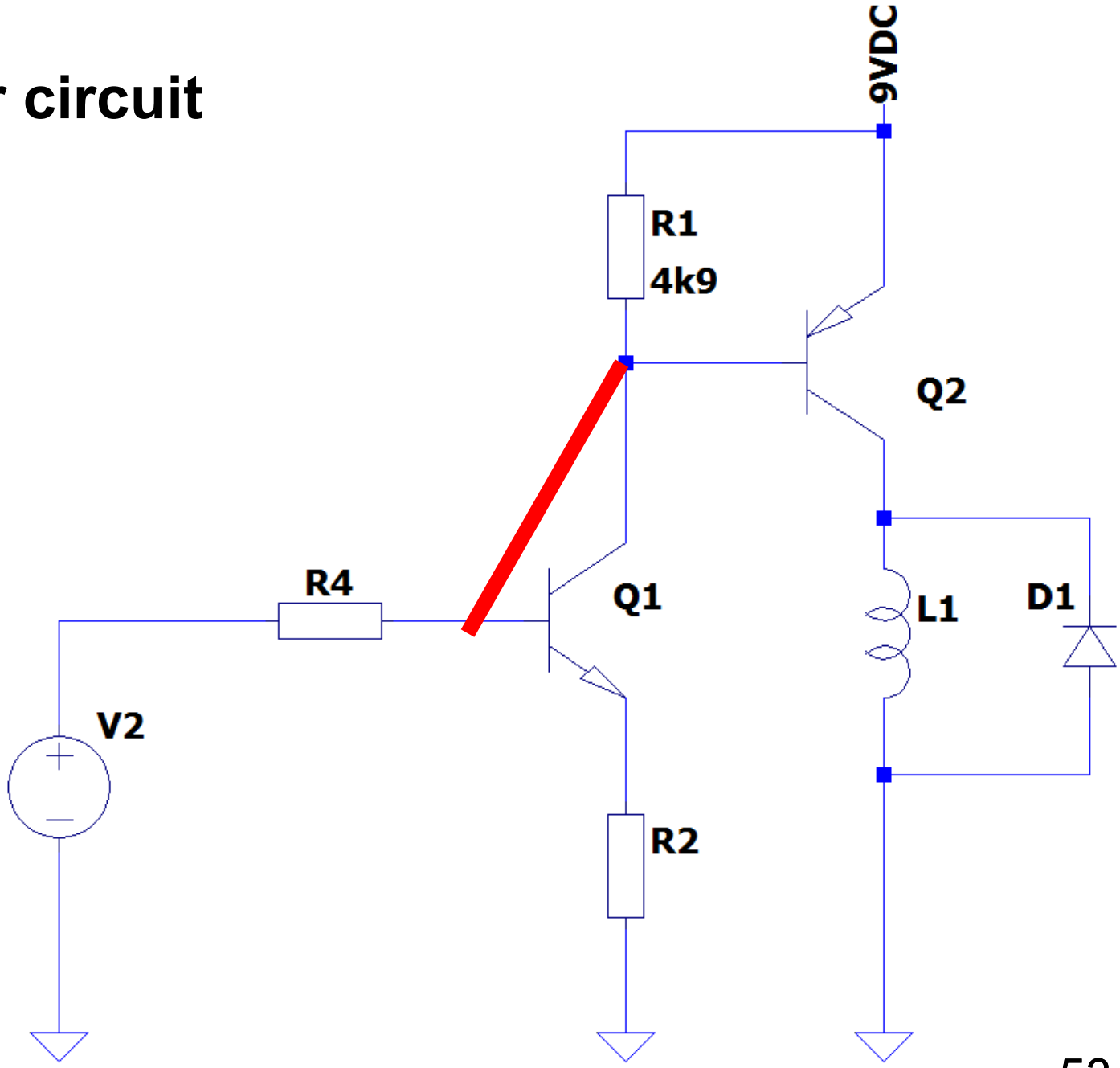
Transistor circuit



Transistor circuit

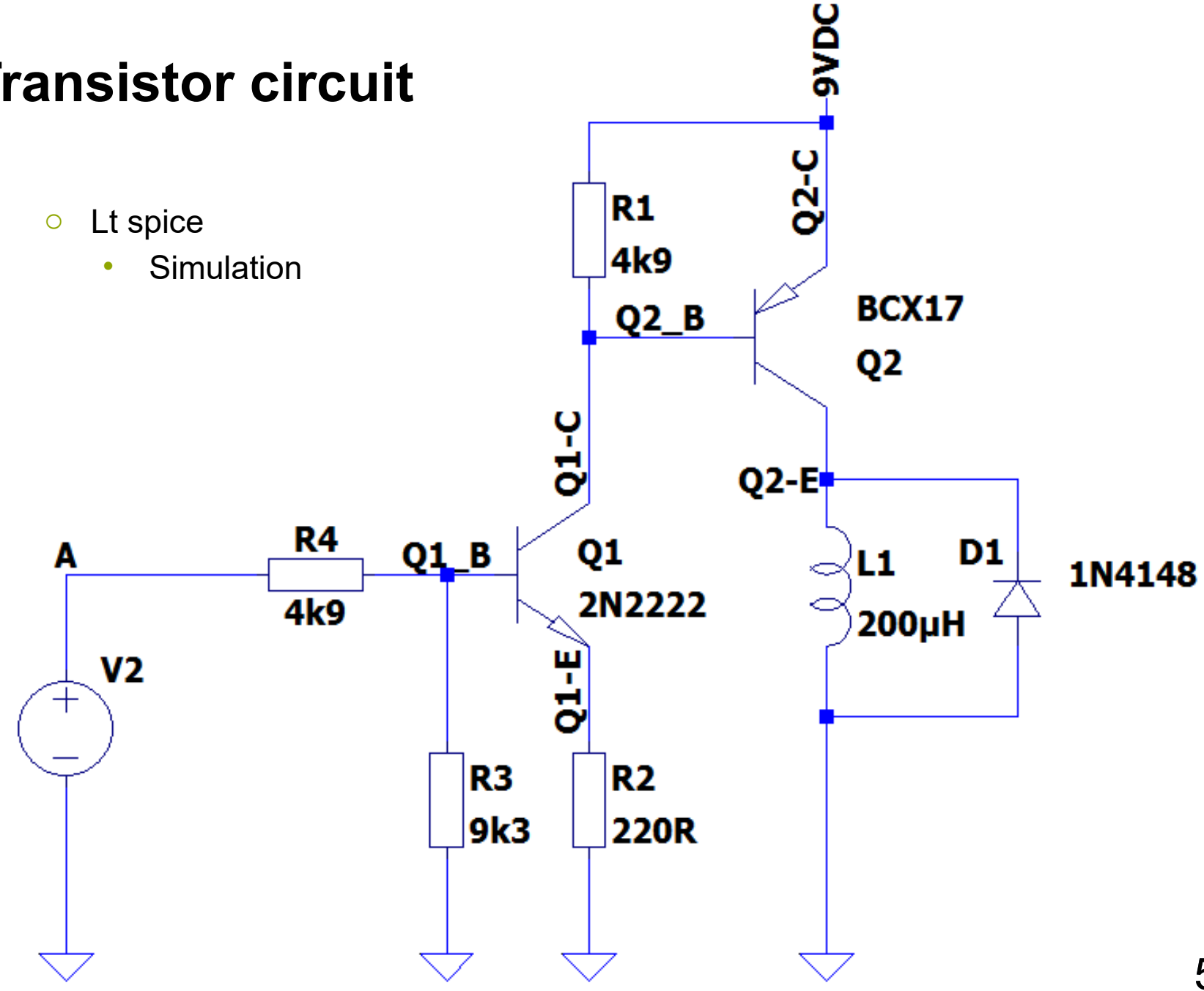


Transistor circuit



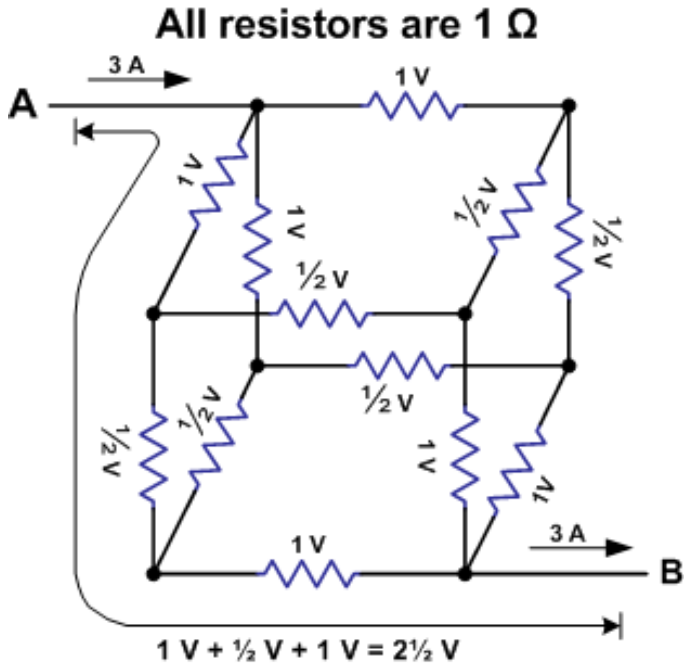
Transistor circuit

- Lt spice
  - Simulation



Simulation results

- Measurement:
  - Resistor I1
  - **5000 0.322**
  - **10000 0.321**
  - **15000 0.318**
  - **20000 0.236**
  - 25000 0.167
  - 30000 0.128
  - 35000 0.107
  - 40000 0.093
  - 45000 0.082
  - 50000 0.072



Exhaustive testing

- Exhaustive testing
  - TDS & EC meter
  - Siemens = 1/R
  - Tested dozens of liquids


Kruidvat
afwasmiddel
produit vaisselle
ultra concentrated
Men
shower
curry gewurz
Remia
24h
NIVEA SUN
after sun hydrate
TEX MEX
TACO SAUCE
elmex
SENSITIVE
NIVEA
Repair
Franse Mosterd
205g
E3645 China

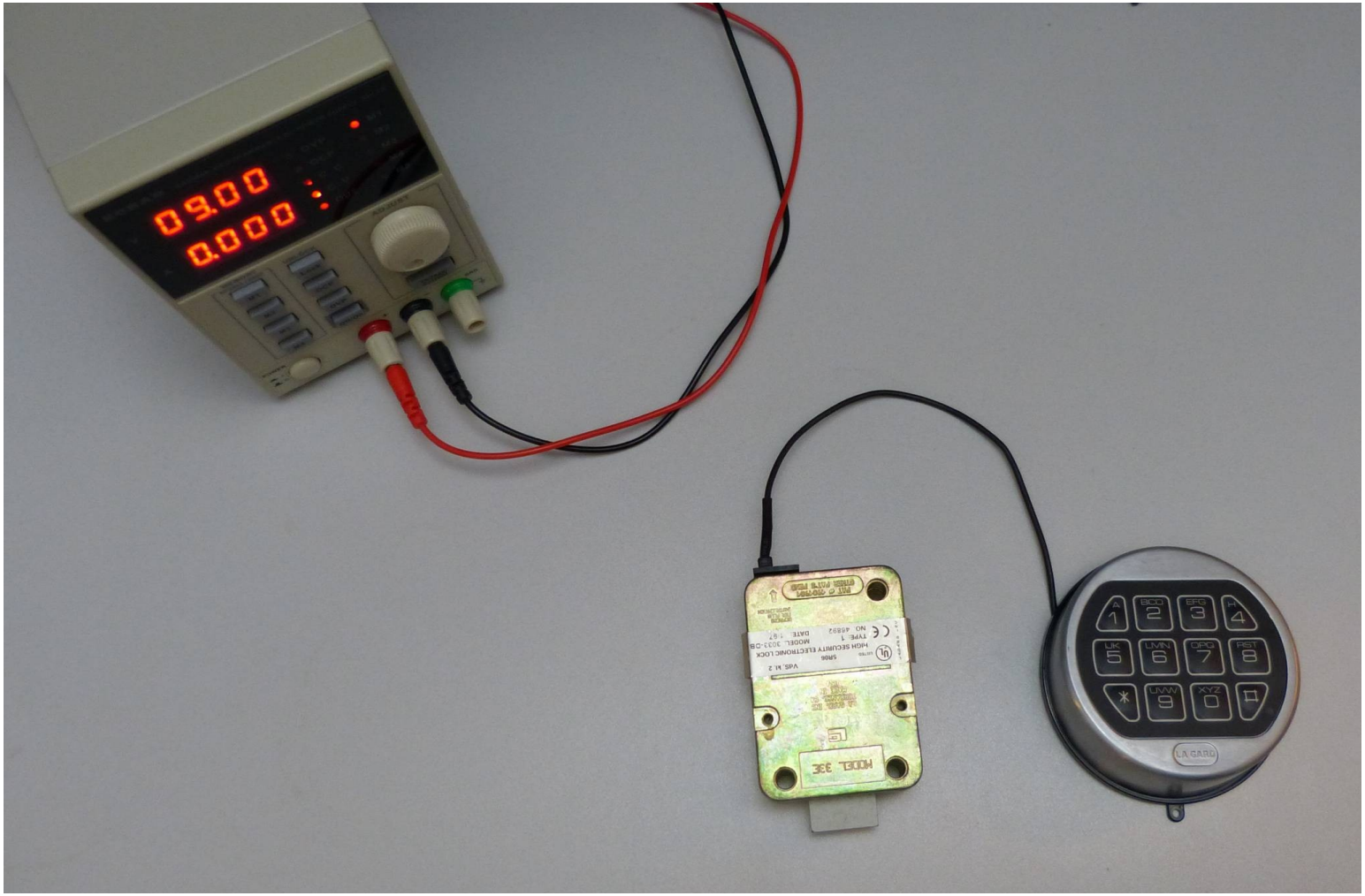
Exhaustive testing

riscure

- Close enough:
  - Coctail sause
  - Ketchup
  - Curry
  - Garlic sause
  - Shower gel

Demo: Opening a safe lock with Ketchup

riscure

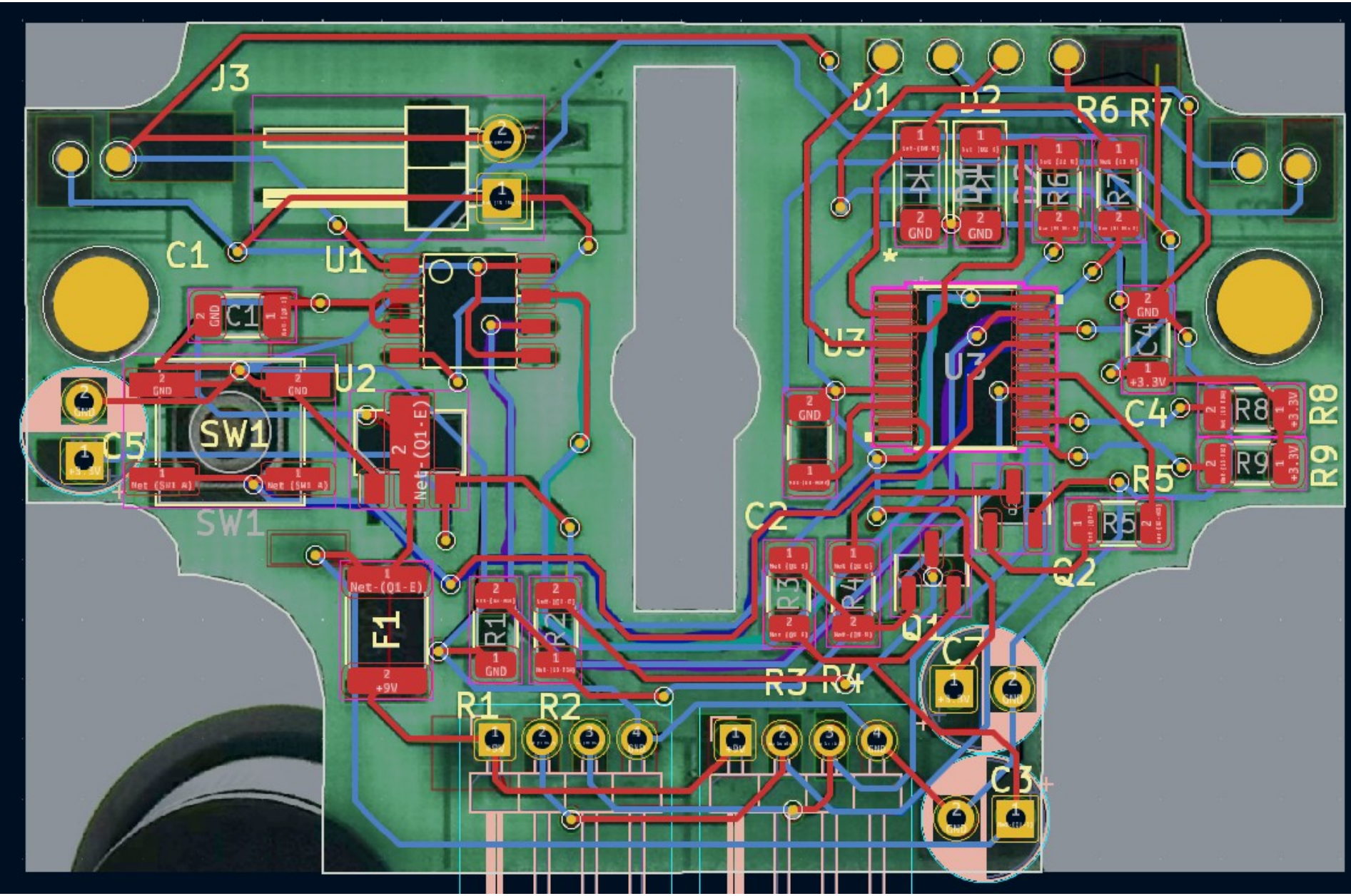


riscure

Wrapping up


1 A
2 BCD
3 EFG
4 H
5 IJK
6 LMN
7 OPQ
8 RST
*
9 UVW
0 XYZ
#


AMBITION

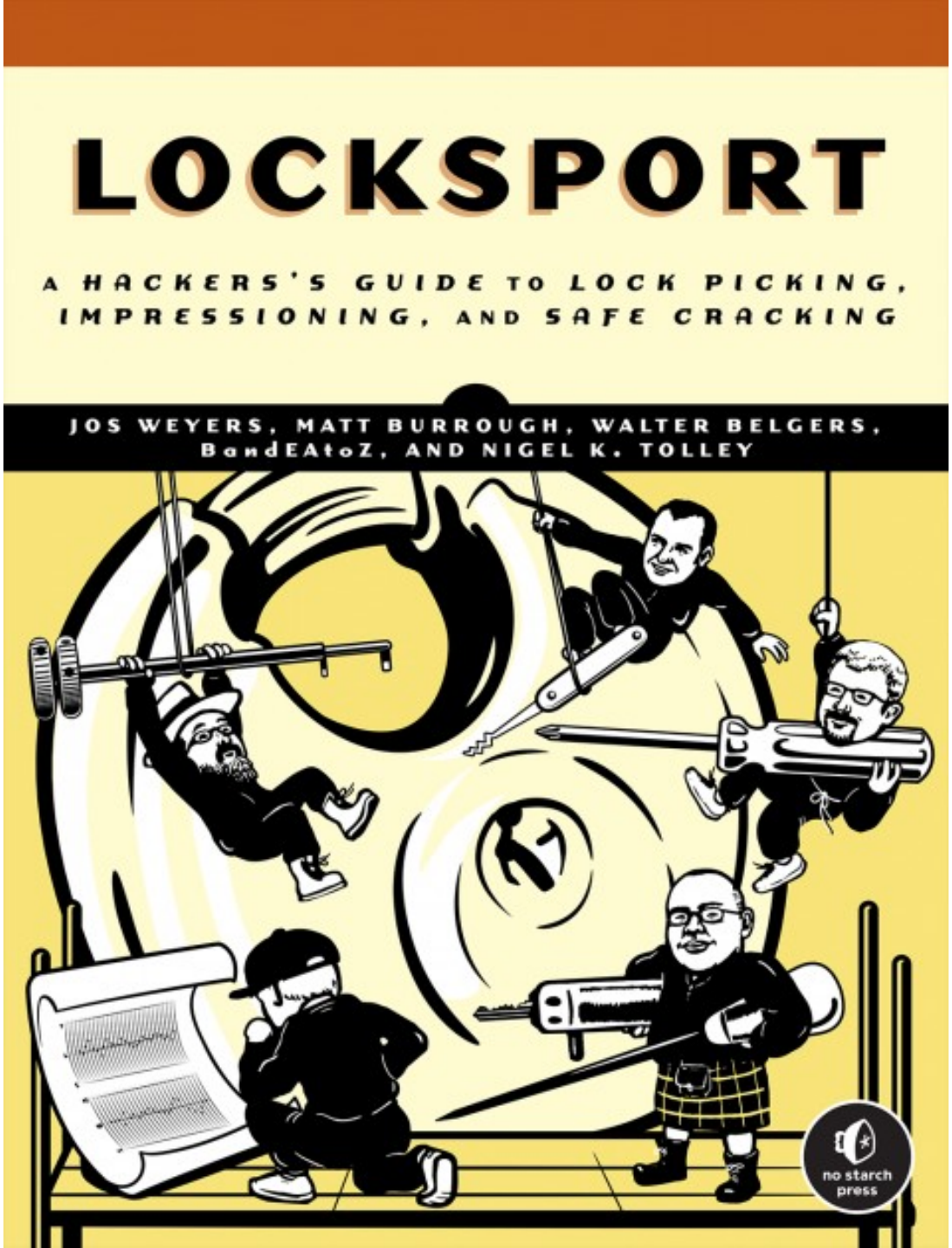


Devo over at Lockpickers United

Other's work

- Plore
  - Side-channel attacks on high-security electronic safe locks
  - DEF CON 24
  - https://www.youtube.com/watch?v=lXFpCV646E0
- Michael Huebler
  - The KABA MAS X-09 High Security Safe Lock
  - Oktober 2008
  - https://toool.nl/Publications
- Mike Davis
  - No Mas
  - https://www.youtube.com/watch?v=viU8Qs1Sccg
  - DEF CON 27
- Lance H. Mayhew Jr.
  - Electronic Safe Locks And How To Defeat Them
  - 2019

riscure


LOCKSPORT
A HACKER'S GUIDE TO LOCK PICKING, IMPRESSIONING, AND SAFE CRACKING
JOS WEYERS, MATT BURROUGH, WALTER BELGERS, BondEAtoZ, AND NIGEL K. TOLLEY
no starch press