Electronic safe locks

14th of October

LockCon 2023

Jan-Willem

Motivation

riscure

EE -> EE -> SA

- Designing electronics
- Analysing security of embedded systems
- Teaching

Lockpicking

- Community: Toool, Hackerspaces, Online
- Sharing knowledge: Blackbag, workshops
- Research: Whatever has my interest

Cutaways, and lever locks

When we teach lockpicking we usually revert to schematics of locks, and different models for demonstrating the functionality of locks. Usually required as the core functionality is well hidden, and not often observable in action. Multiple skilled machinists have made cutaway locks for the purpose of demonstrating the inner workings of real locks.

At one cutaway themed evening, we had over 50 unique cutaways on the table. From all brands and mechanisms. Some of which even the pins themselves were cutaway.

Search for:
Search

Recent Posts
- LockCon 2023 Schedule

Recent Comments
No recent comment found.

Categories
- Lockpicking
- Keys
- Locks
- Impressioning
- Uncategorized
- General
- LockCon
- Conference
- Decoding
- Gatherings

Meta
- Log in
- Entries feed
- Comments feed

riscure

Electronic safe locks

Introduction

Electronic locks

Electronic locks the ideal target?

- Usually uninteresting
- Not designed with security in minded
- Low impact
- RFID, BLE, mobile apps
- Unobtainable or expensive
  - Cliq
  - XT
  - Cyberkey

Electronic locks

Electronic safe locks are different story

- Small attack surface
- Standalone
- Good basis for security
- Hardware attacks
- Affordable

Electronic safe locks

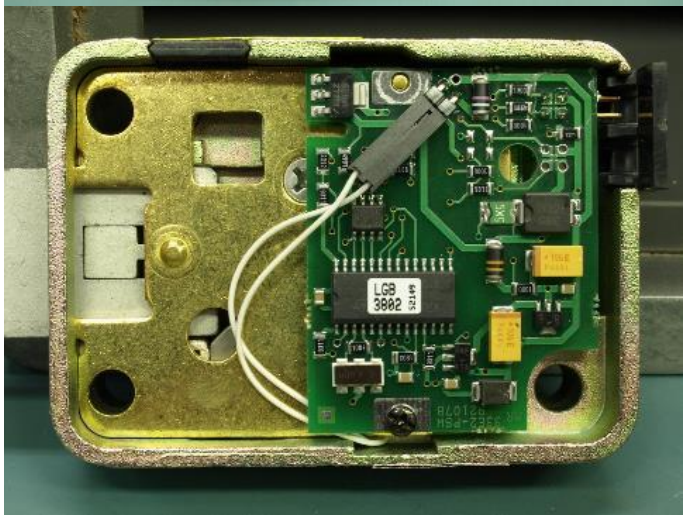
- Force multiplicatation
- Secure by design

Safe Door

Electronic safe locks

Consumer / commercial

- Special requirements:
  - UL 2058 Type 1
  - Easy to use
  - Reliable locks for a good price
  - Quality differs



Pictures by eevblog is licensed with CC BY 2.0.

Electronic safe locks

Banking and Pharmacy

- Special requirements:
  - Multi user
  - Auditing
  - Delays
  - 2FA

https://www.dormakaba.com/us-en/solutions/products/safe-locks/axessor/axessor-ip-293124

Electronic safe locks

US Goverment

- Special requirements:
  - FF-L-2740 B
  - EMP proof
  - TEMPEST proof
  - Etc
- Kaba Mas X0 series
  - X07 to X10

Target

Kaba mas X0* locks

- X07 1992
- X08 1998
- X09 2002
- X10 2013
- FF-L-2740B

Asset

- Program content
- Open lock without combination
- Dialled combination
- Settings

INSTALLA
INSTRUCTIO
MODEL X-09 ®
HIGH SECURITY ELECTRONIC LOCK TYPE IF FF-L-2740A
S/N: X09SR0140110620128ARM
COVERED BY U.S. AND FOREIGN PATENTS OTHER PATENTS PENDING
KABA MAS LLC
LEXINGTON KY U.S.A.

riscure

Embedded System Security

Welcome!

ESS Process

Target -> Asset -> Security

Treat modelling

- Attacker, Assets, Vulnerabilities, etc

Vulnerability analysis

- Analyse previous work

Test the potential vulnerabilities with highest impact

- JIL rating

Attacker model

The attacker: Me

- 10y+ lockpicking
- 5y+ Electronics design
- 3y+ Embedded security
- 1000 hours to invest
- Limited access to specialized tools (<10k)
- Full access to basic tools (<1k)
- Knowledge to create custom tools (<1k)
- Access to public knowledge of the target
- Access to 10+ samples
  - Can move laterally between targets
- **Doesn’t give up easily**

Embedded Systems & Security

riscure

Vulnerable to attacks

Logical

Physical

Side-Channel Analysis

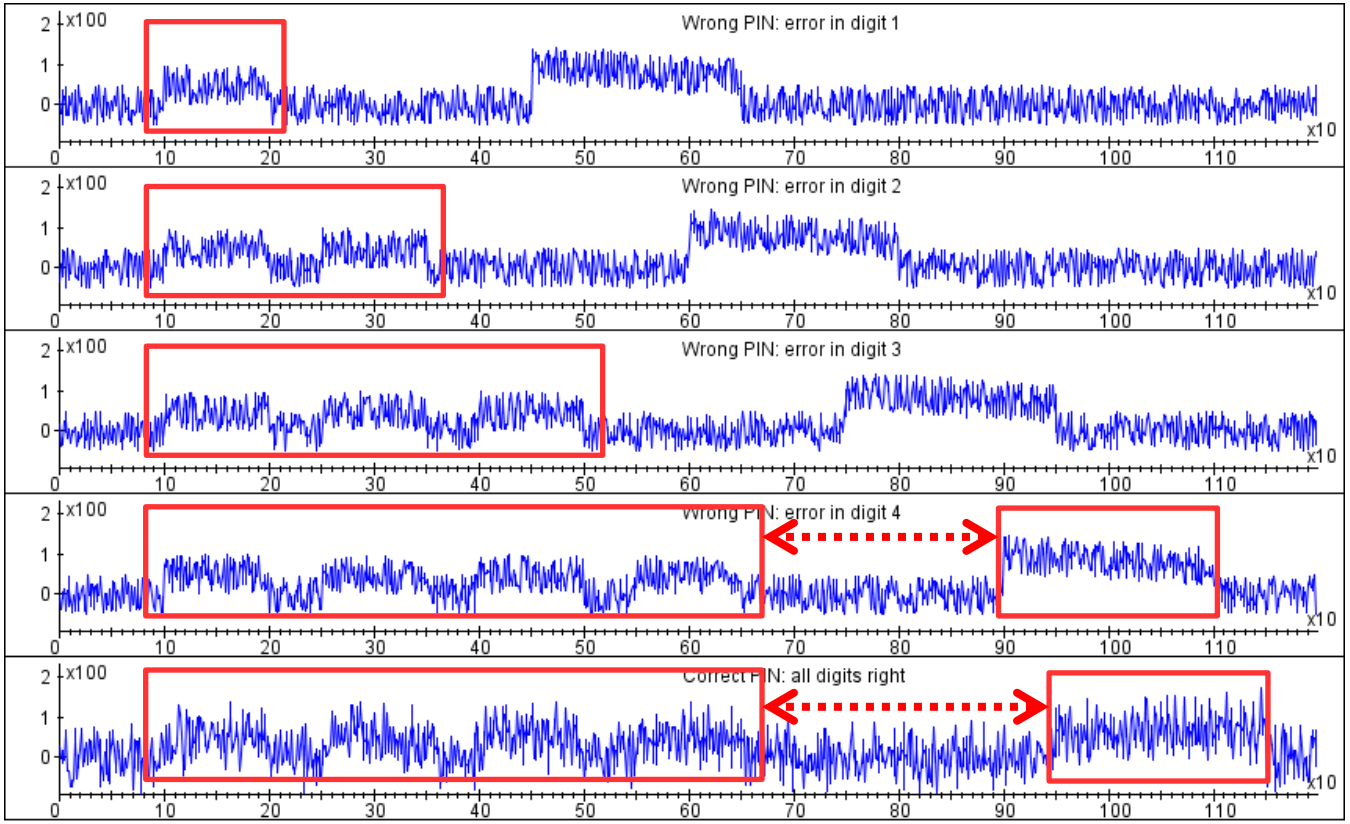
Fault Injection

Simple Power Analysis

riscure

Signal leakage from busses, registers, ALUs, etc.

Example: 4-digit password verification attempts



PWD

????

8???

82??

827?

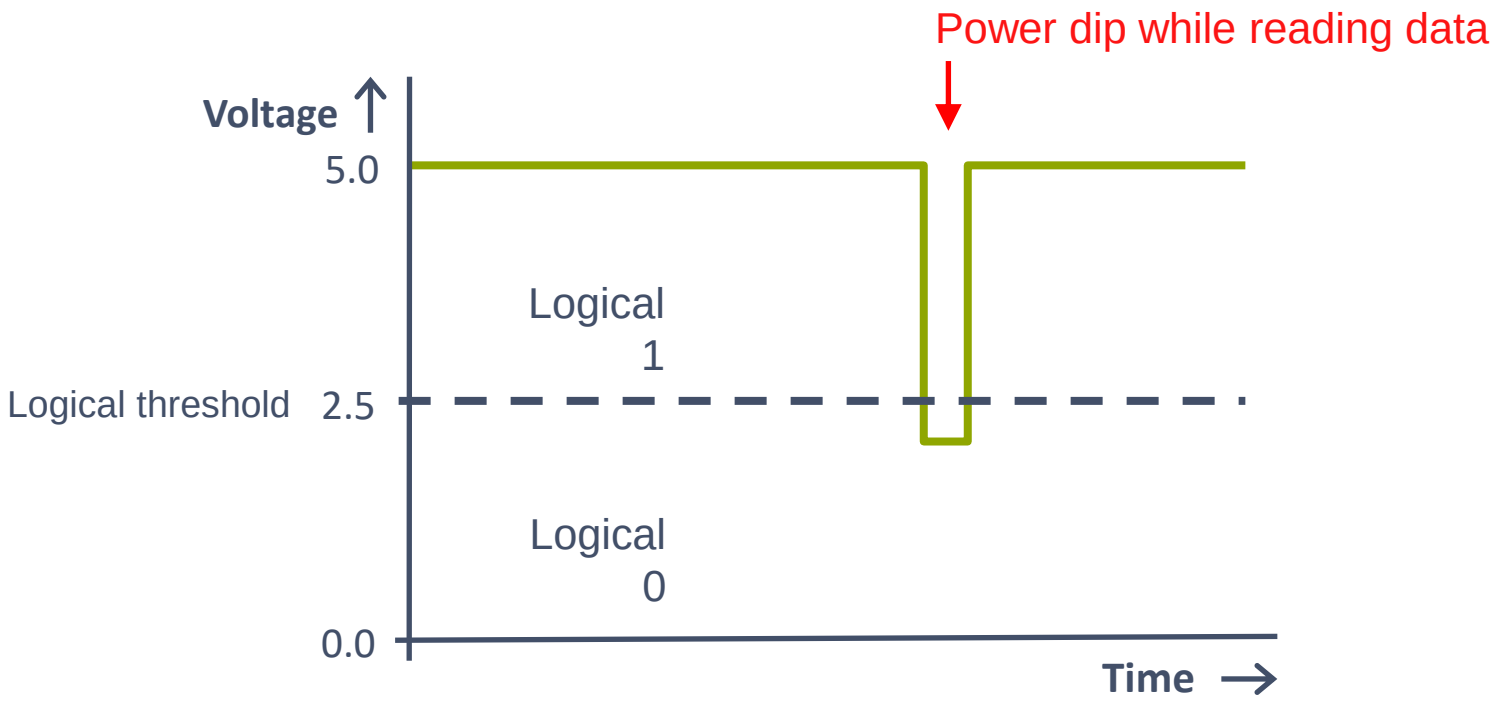
8275

Concept - Glitching

Inject data fault through glitches on power supply or clock

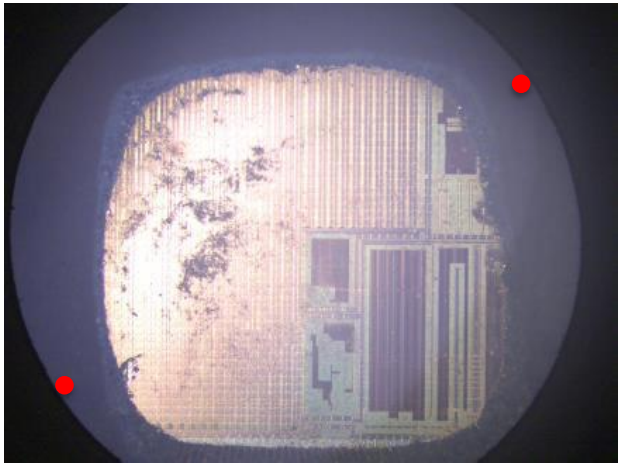
- Stored data (memory)
- Intermediate data (registers, buffers, cache, bus)

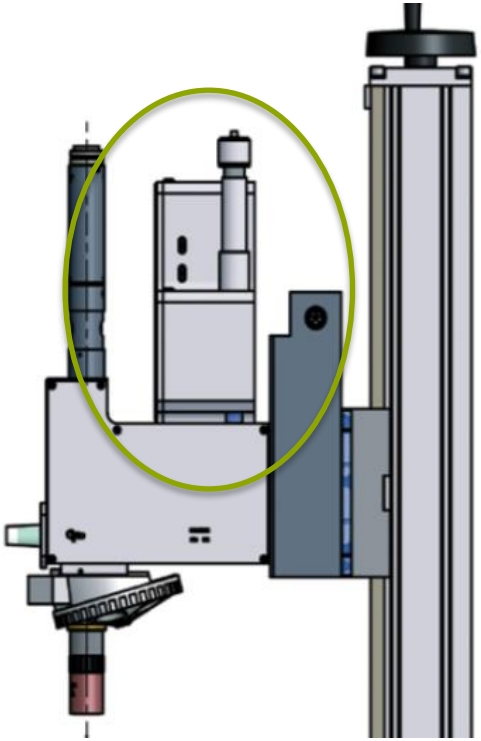
Example:

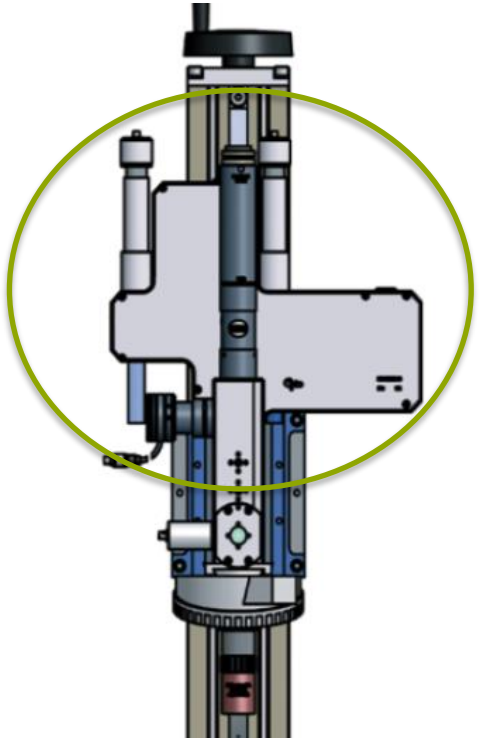


Twin Scan for two laser spots

1. Two laser sources through one microscope objective
2. Each beam can be positioned and both lasers can be fired independently







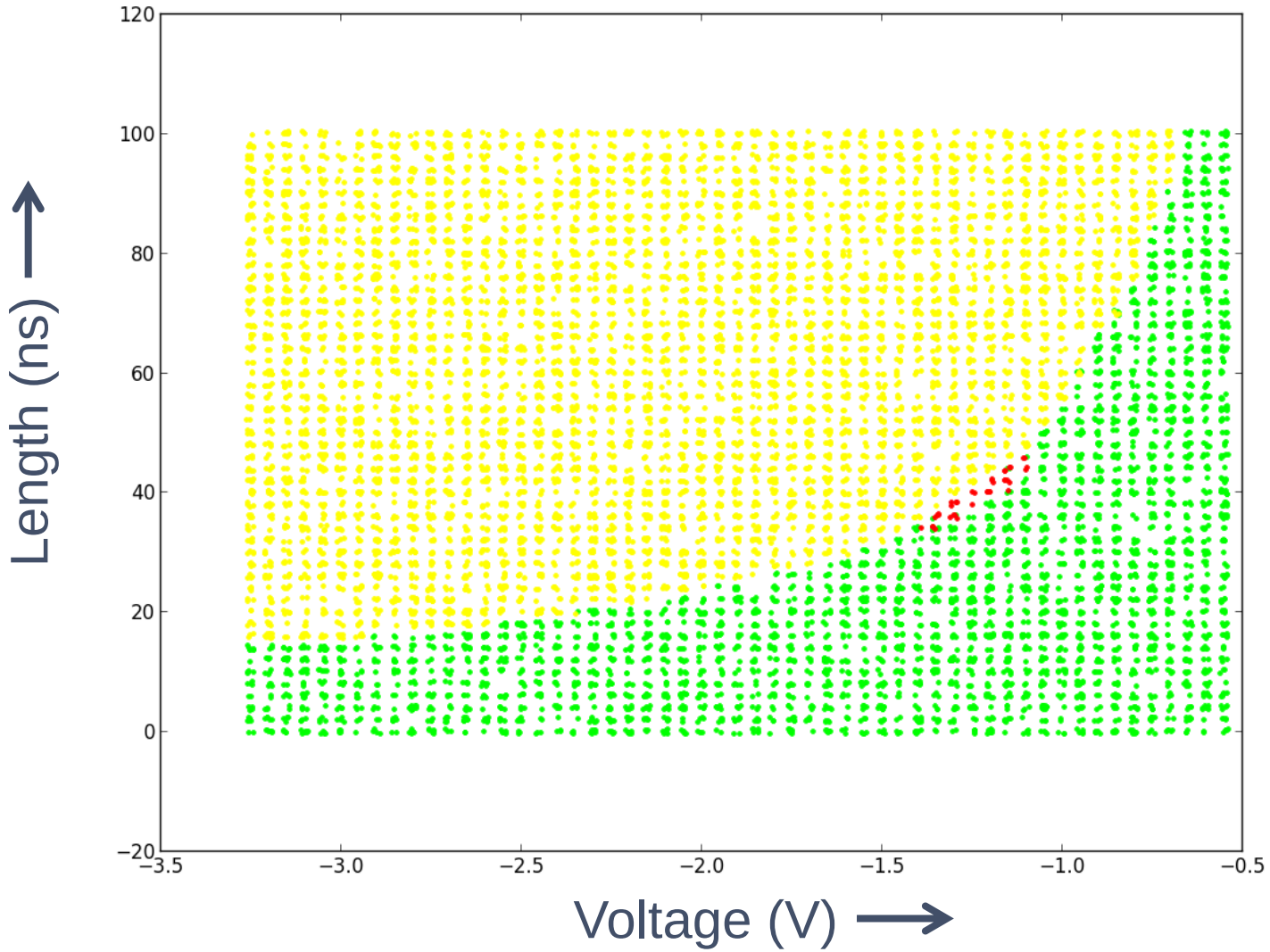
3. Laser spots distance bound by field of view
4. Closed loop control system

← 5x objective, 1x zoom, ∅ 3.6 mm (piñata)

restricted

How to find the right parameters?

riscure



riscure

Electronic safe locks

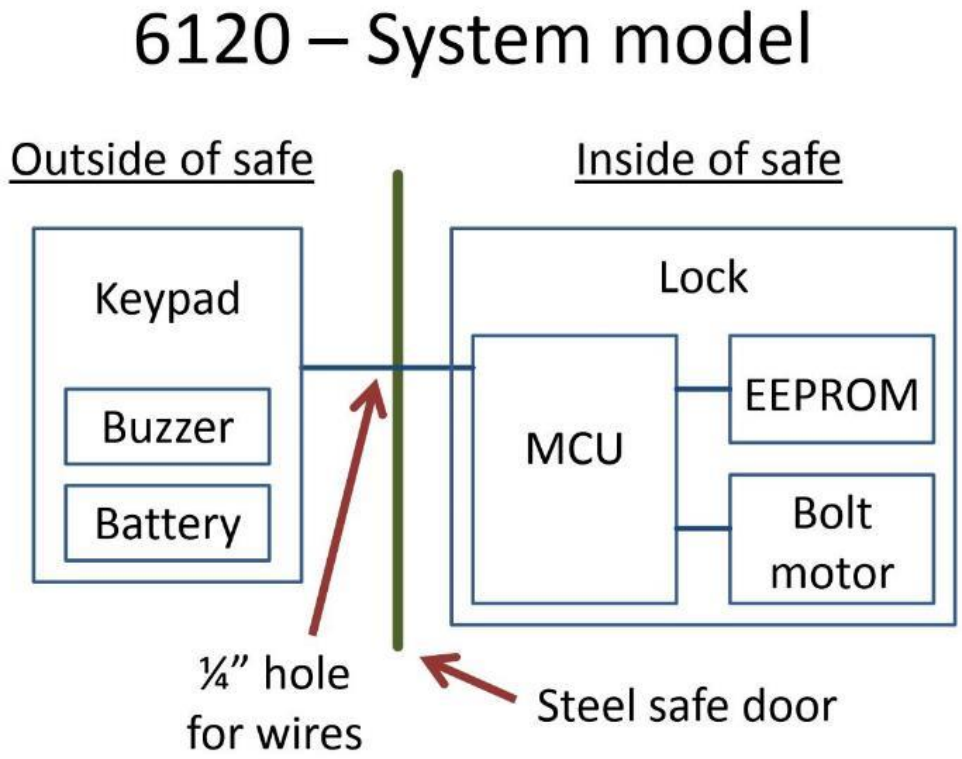
Previous work

Published Attacks

Side-channel attacks on high-security electronic safe locks

- Plore, 2016
- Defcon 24
- https://www.youtube.com/watch?v=lXFpCV646E0

Published Attacks: Plore Defcon 24

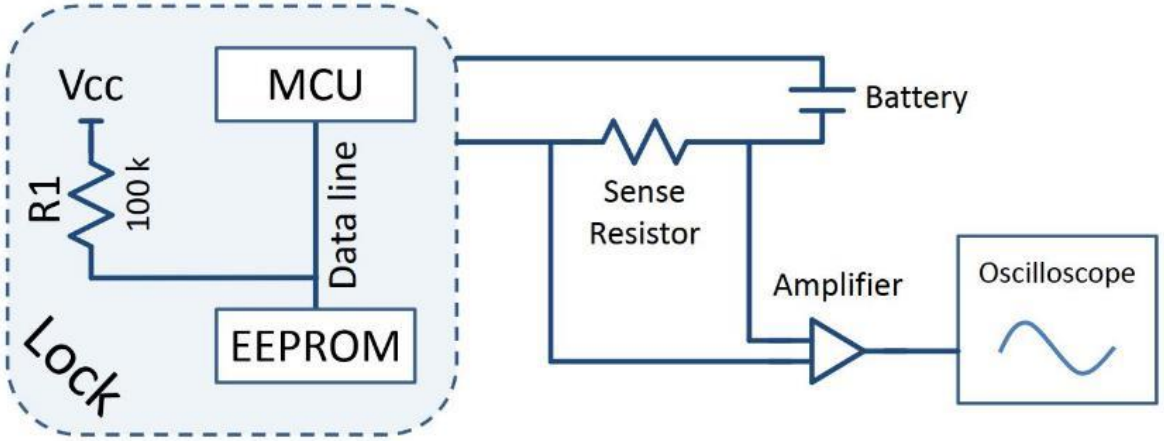


https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20Plore-Side-Channell-Attacks-High-Security-Locks-UPDATED.pdf

Published Attacks: Plore Defcon 24

riscure

6120 – Circuit model



Bit value	Data line volts	Volts *across* R1	Current through R1
1	5 volts	0 volts	0 µA
0	0 volts	5 volts	50 µA

∴ Higher current consumption means the bit being read from EEPROM is a 0, and a lower current means the bit is 1

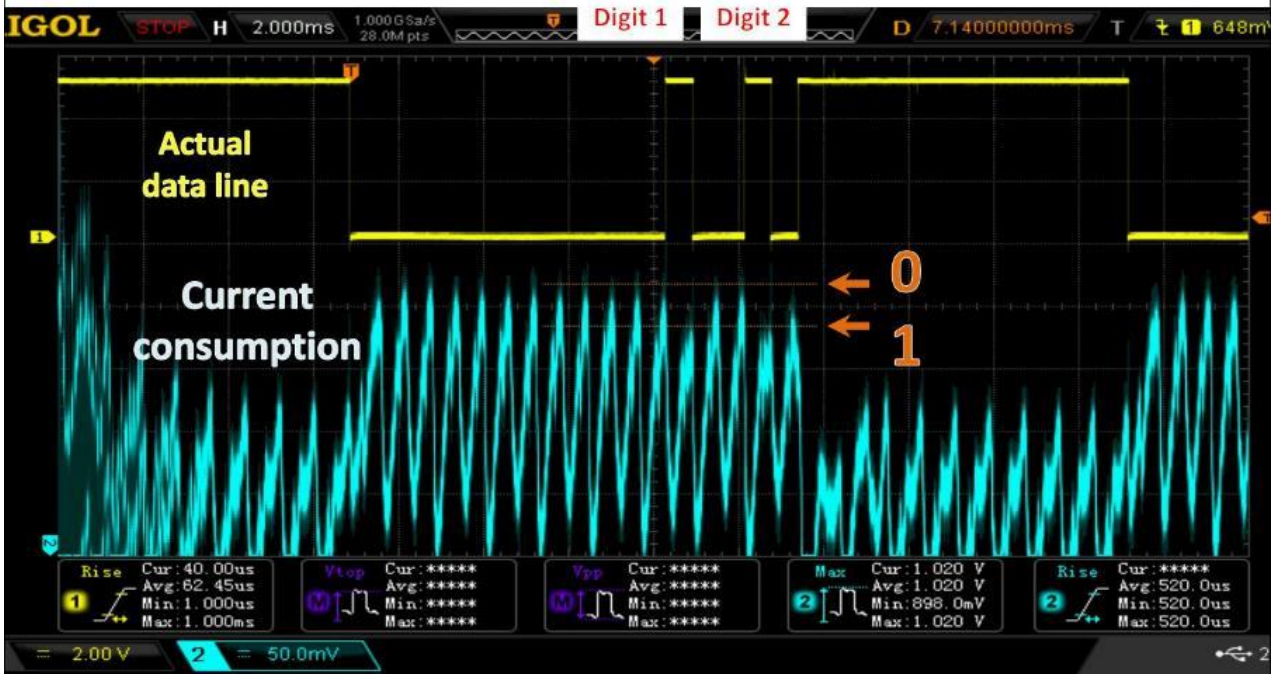
https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20Plore-Side-Channell-Attacks-High-Security-Locks-UPDATED.pdf

Published Attacks: Plore Defcon 24

riscure

6120 – Power analysis

- 1 nibble per keycode digit
- Only lower byte in each EEPROM word is used



https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20Plore-Side-Channell-Attacks-High-Security-Locks-UPDATED.pdf

Published Attacks

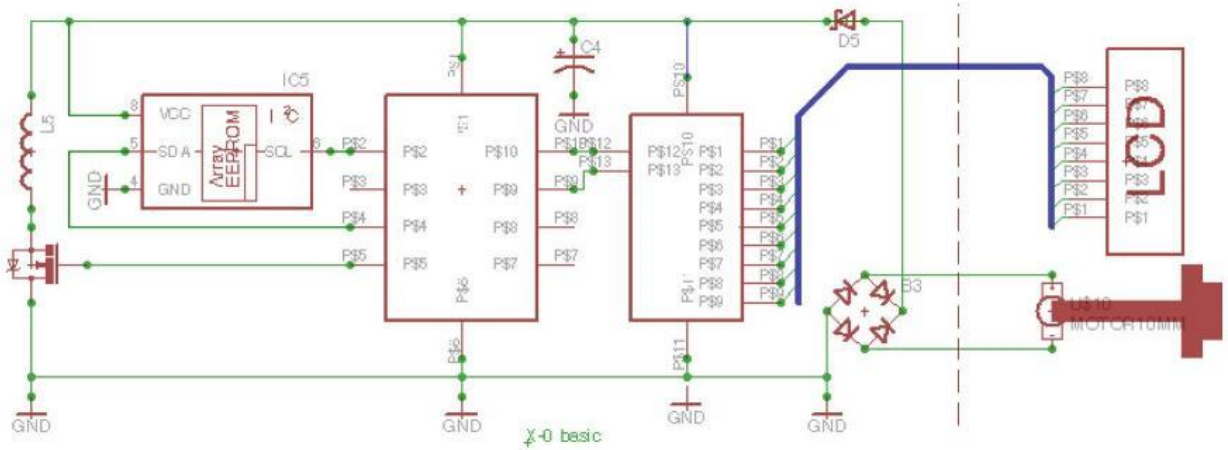
No MAS: (misadventures in high security locks)

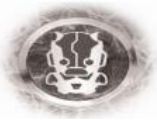
- Mike Davis, IOActive, 2019
- Defcon 27
- https://www.youtube.com/watch?v=viU8Qs1Sccg

Published Attacks: Mike Defcon 27

riscure

IOActive
Hardware | Software | Wetware
SECURITY SERVICES



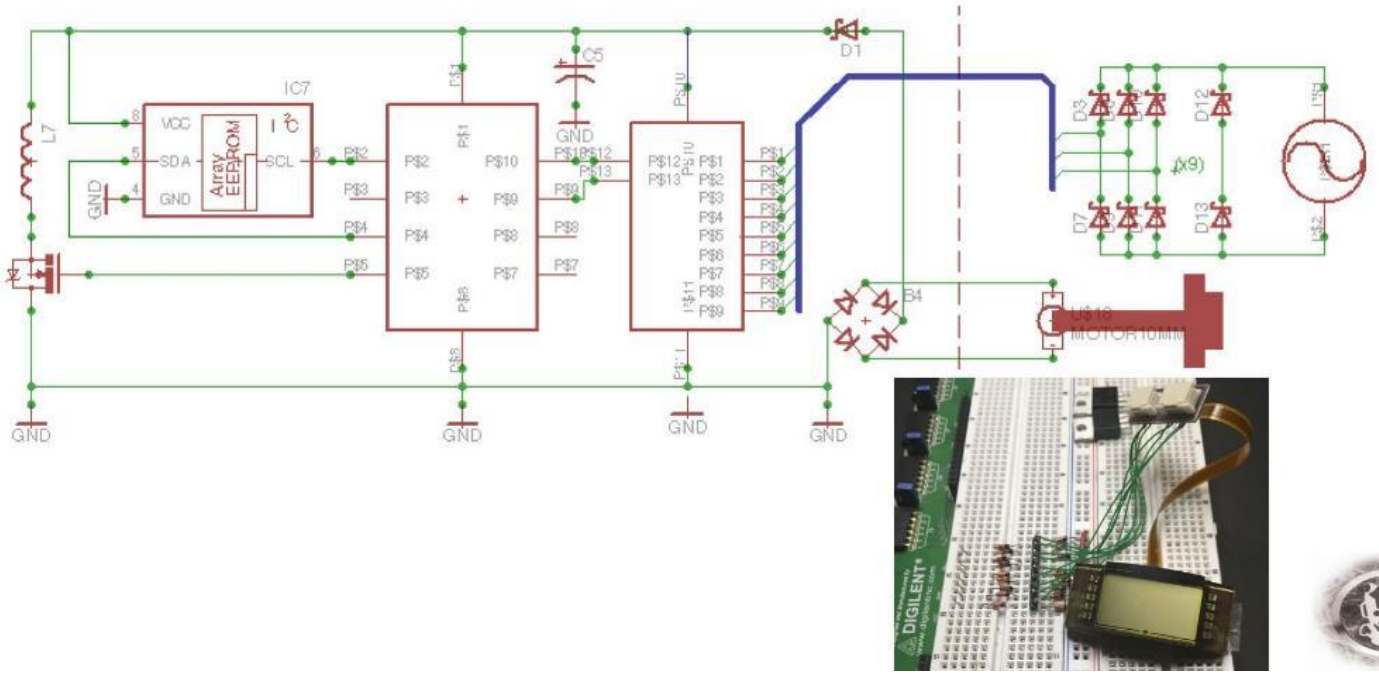


https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Phar-No-Mas-How-One-Side-Channel-Flaw-Opens-Atm-Pharmacies-and-Government-Secrets-Up-to-Attack.pdf

Published Attacks: Mike Defcon 27

riscure

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

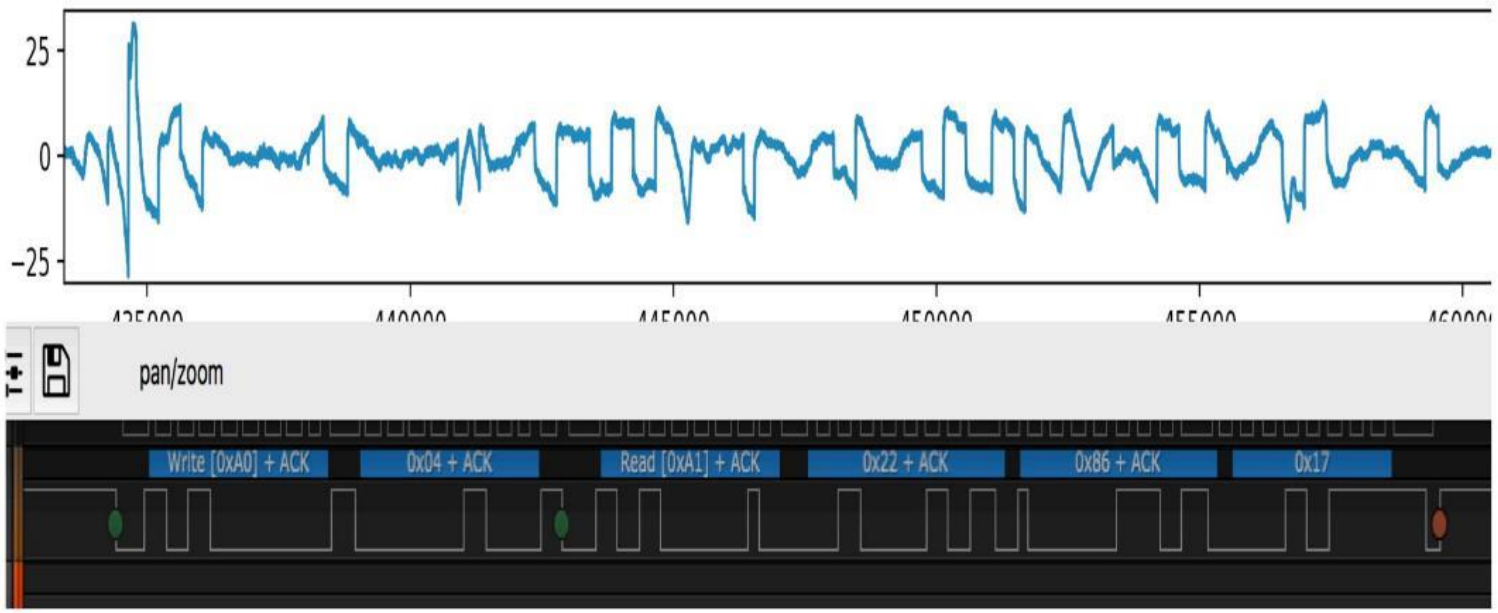


https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Phar-No-Mas-How-One-Side-Channel-Flaw-Opens-Atm-Pharmacies-and-Government-Secrets-Up-to-Attack.pdf

Published Attacks: Mike Defcon 27

riscure

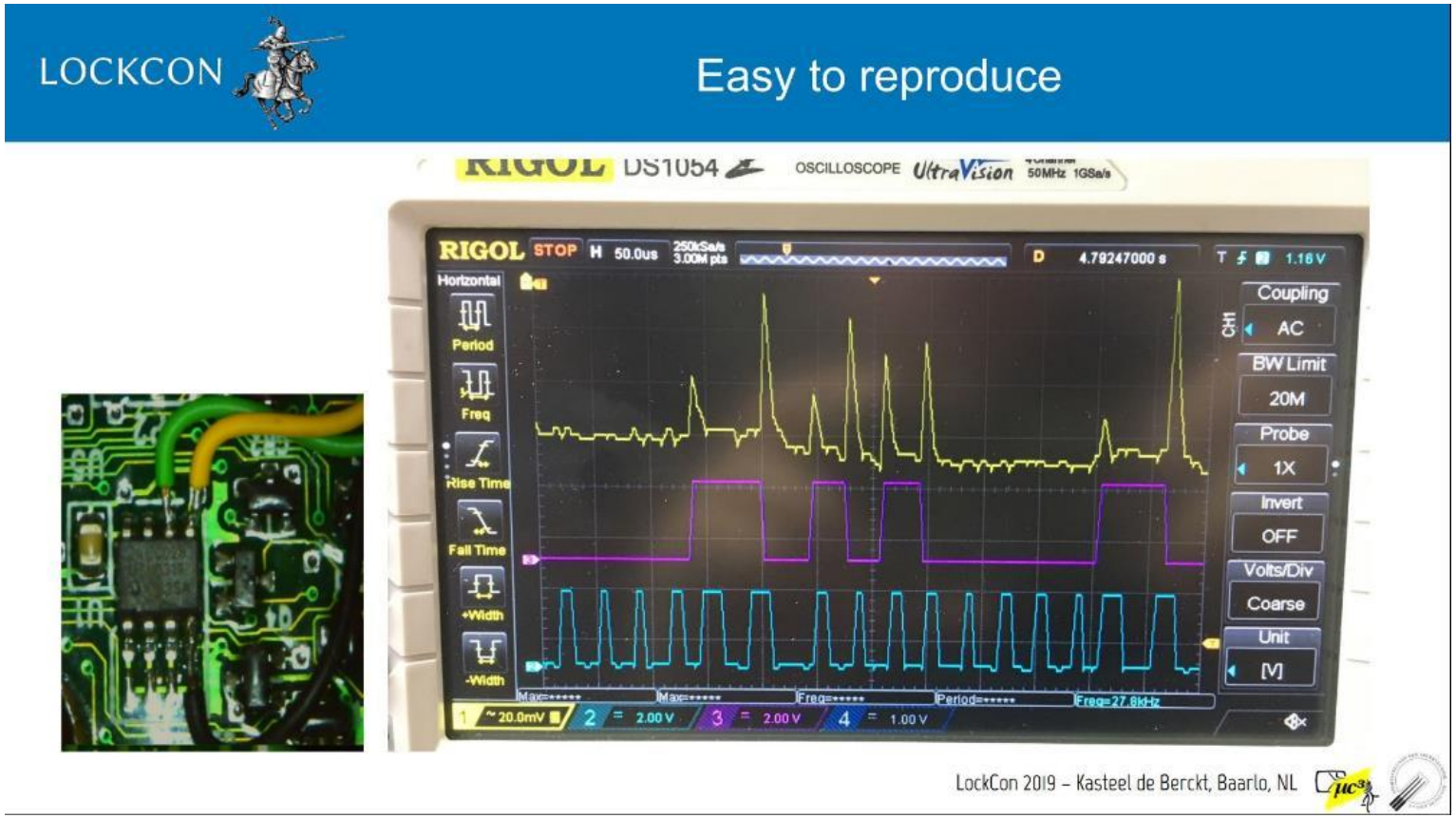
IOActive
Hardware | Software | Wetware
SECURITY SERVICES



https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Phar-No-Mas-How-One-Side-Channel-Flaw-Opens-Atm-Pharmacies-and-Government-Secrets-Up-to-Attack.pdf

Published Attacks: Michael Heubler

riscure

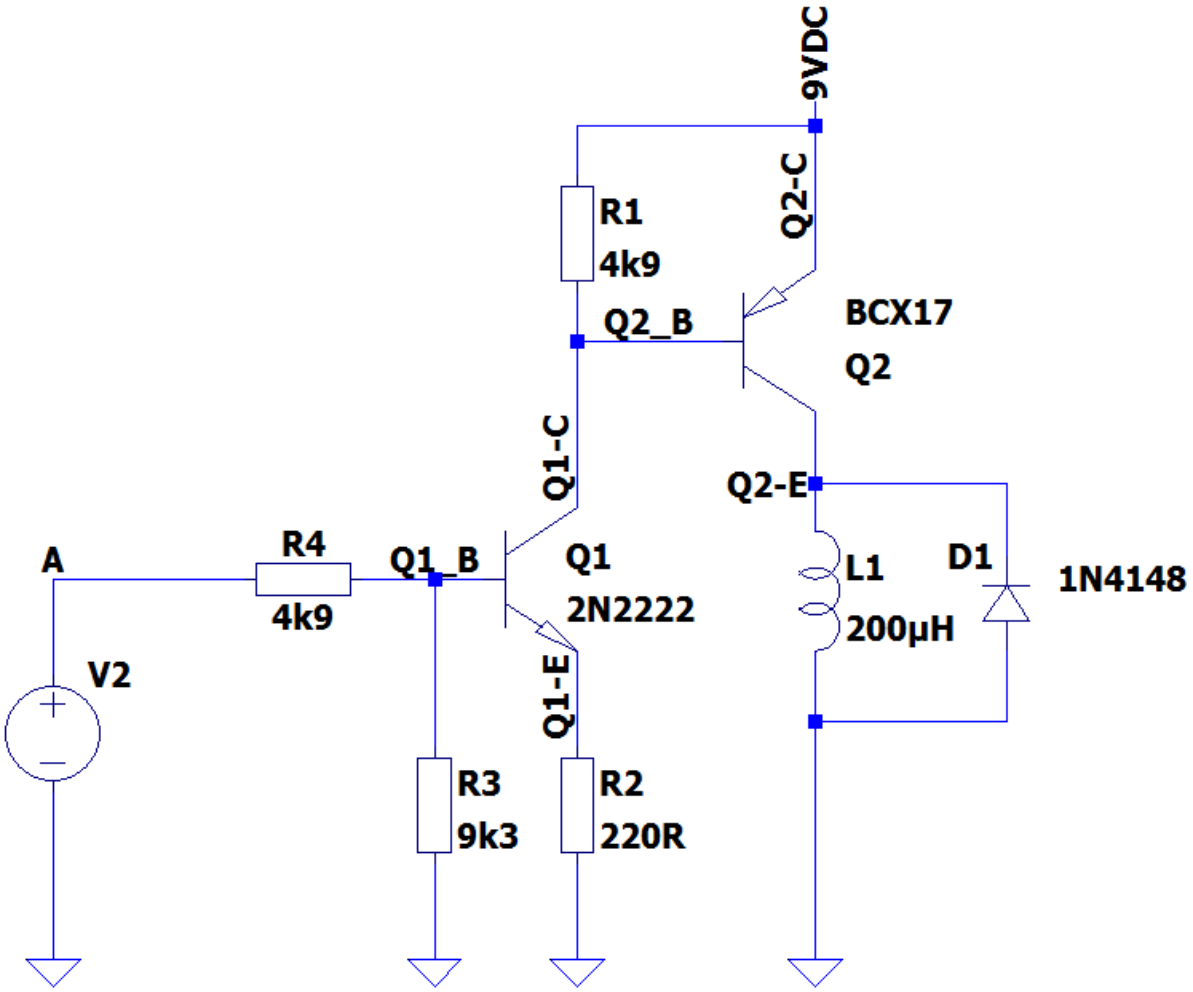


https://toool.nl/media/LockCon_2019_mh_Bluetooth_Locks_and_X-09_update.pdf

Published: Jan-Willem LockCon ’18

riscure

E shock

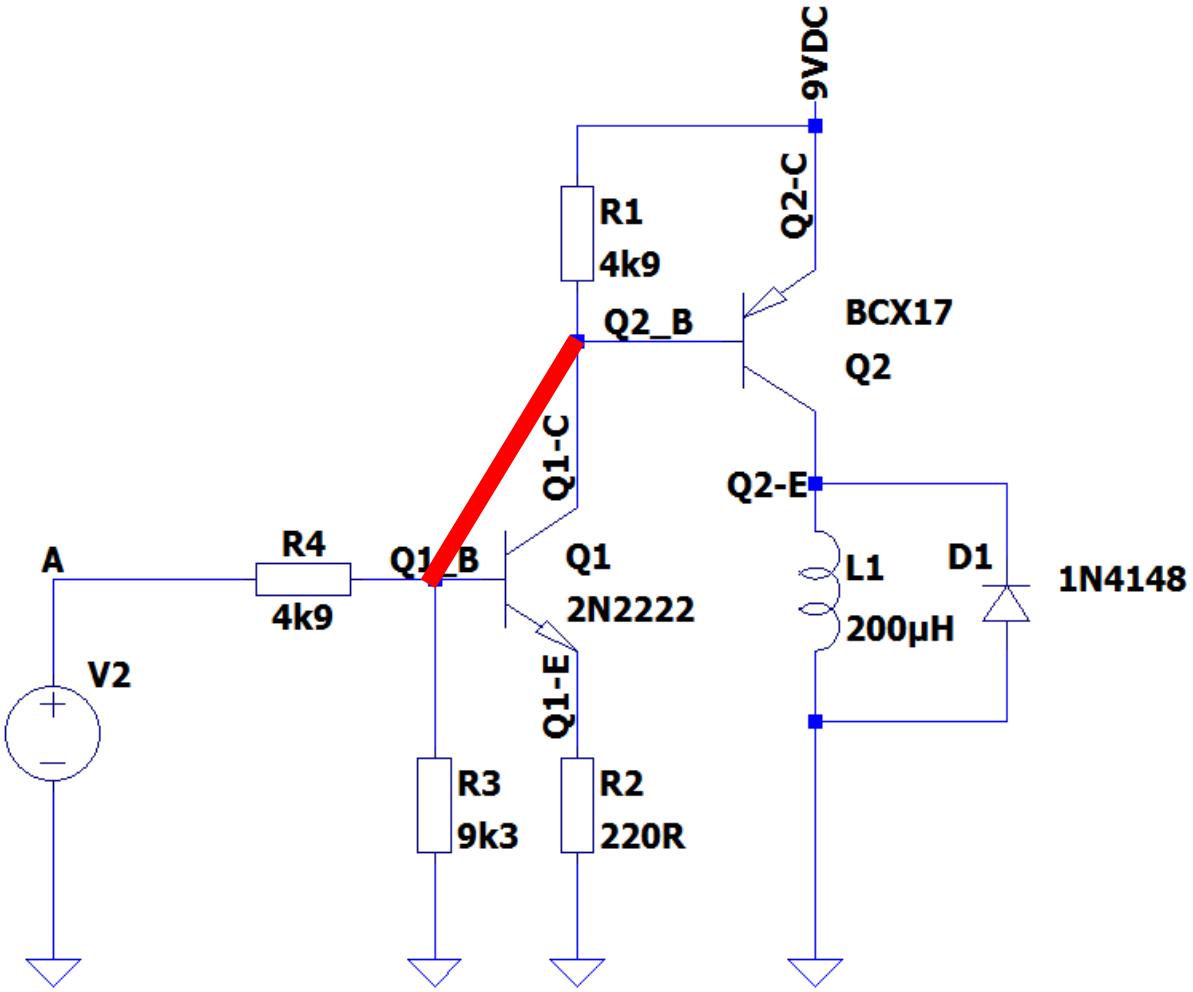


Published: Jan-Willem LockCon ’18

riscure

E shock

- 5k to 20k ohm



Published: Jan-Willem LockCon ’18

riscure

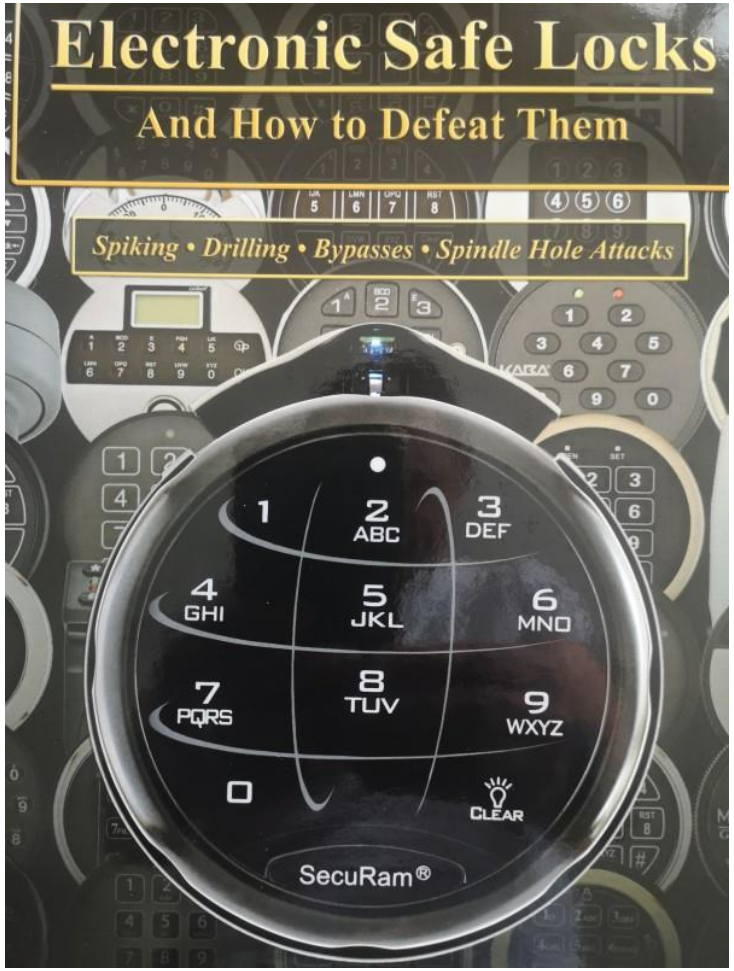
Close enough

- Cocktail Sause
- Ketchup
- Curry
- Garlic Sause
- Shower gel

Published Attacks

Book

- Electronic Safe Locks
  - **Lance Mayhew**



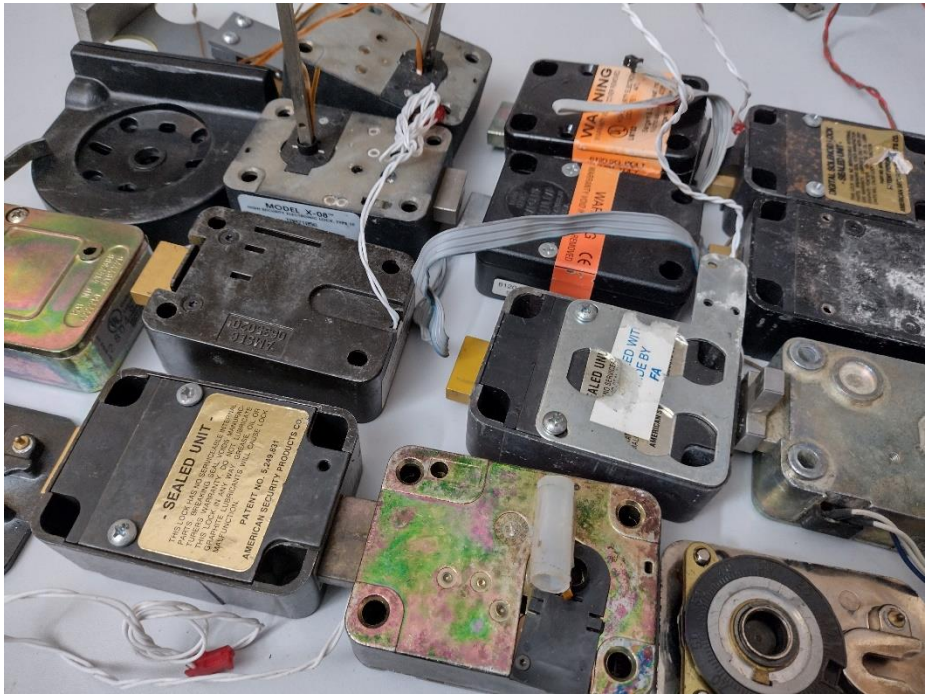
riscure

Novel work on the X0 locks

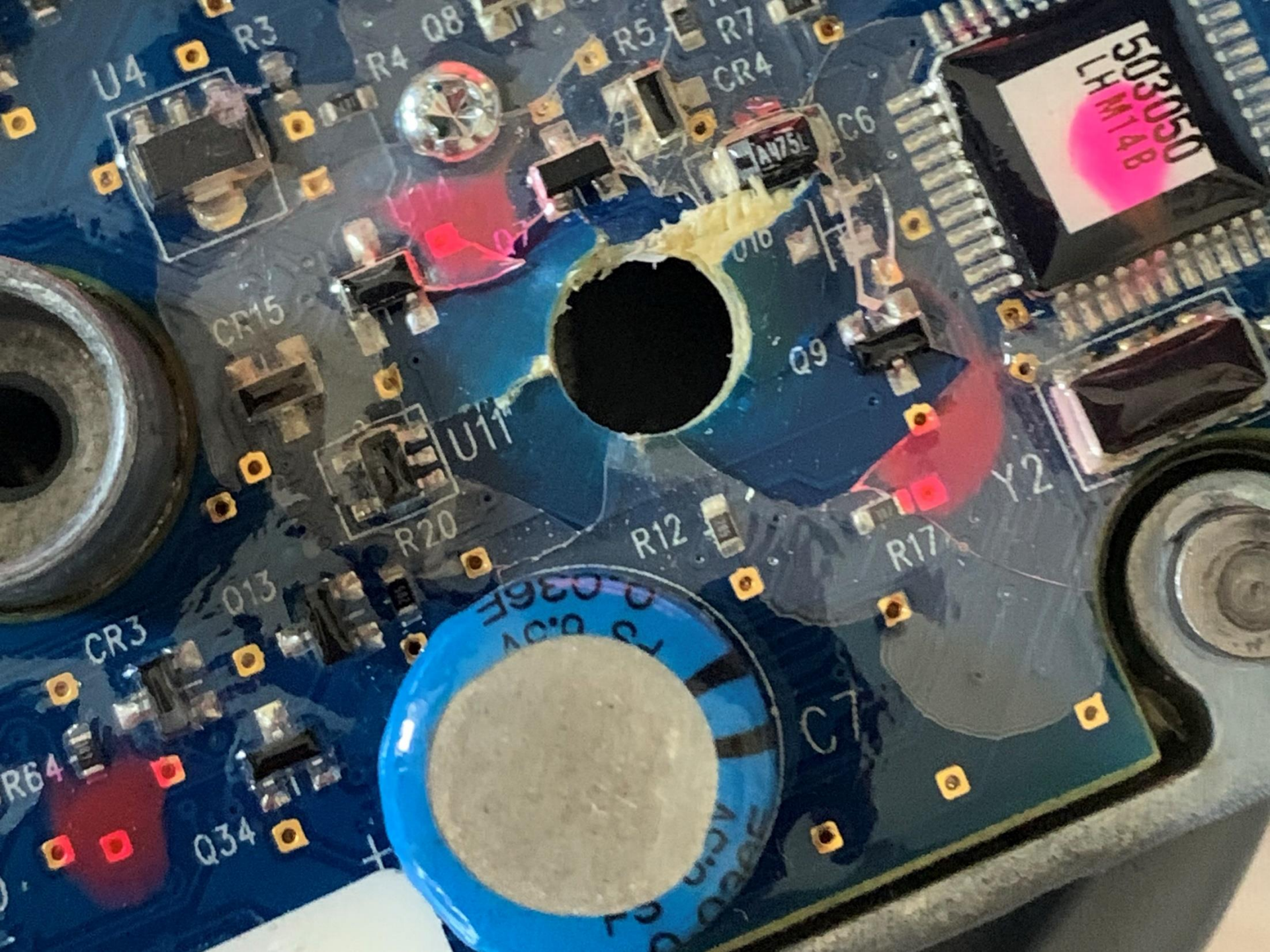
Hurdle: Access to samples

Samples from the USA

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




X-09™
Type 1F
HIGH SECURITY ELECTRONIC LOCK
ITEM NUMBER
10-087
GENERAL SERVICES ADMINISTRATION
APPROVED
SECURITY CONTAINER
HAMILTON
PRODUCTS GROUP, INC.


U4
R3
R4
Q8
R5
R7
CR4
C6
5030S0
LHM14B
CR15
U11
Q9
R20
R12
R17
Y2
CR3
Q13
C7
R64
Q34

Hardware Reverse engineering

riscure

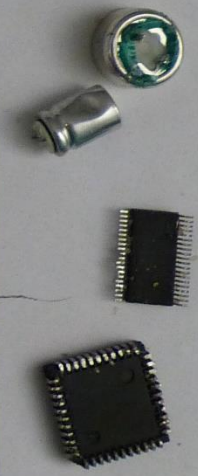
HWRE

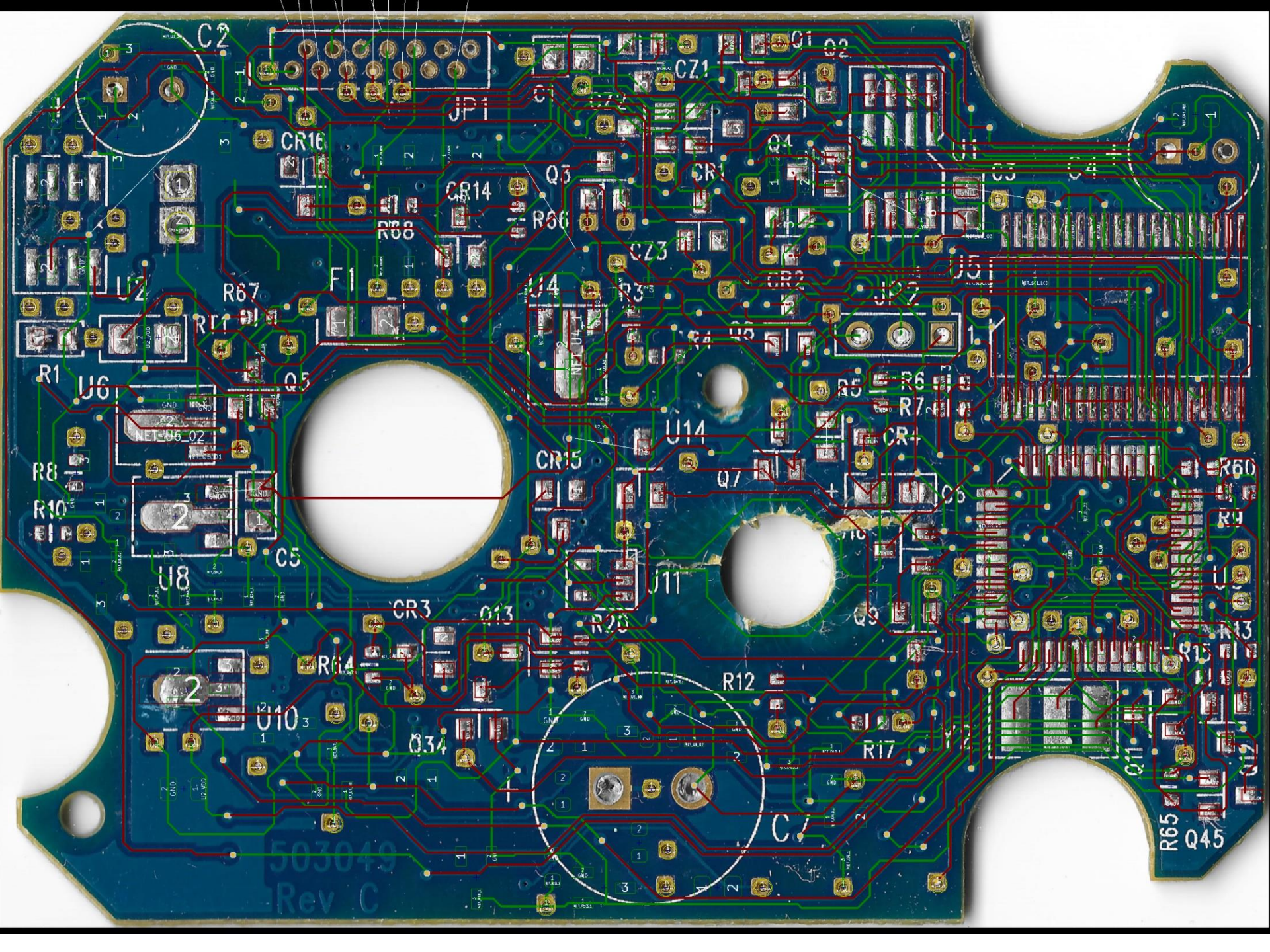
- Slow progress over a year
- Willing to know too many details
- Focussed on all X0* at the same time
- Required to learn HWRE

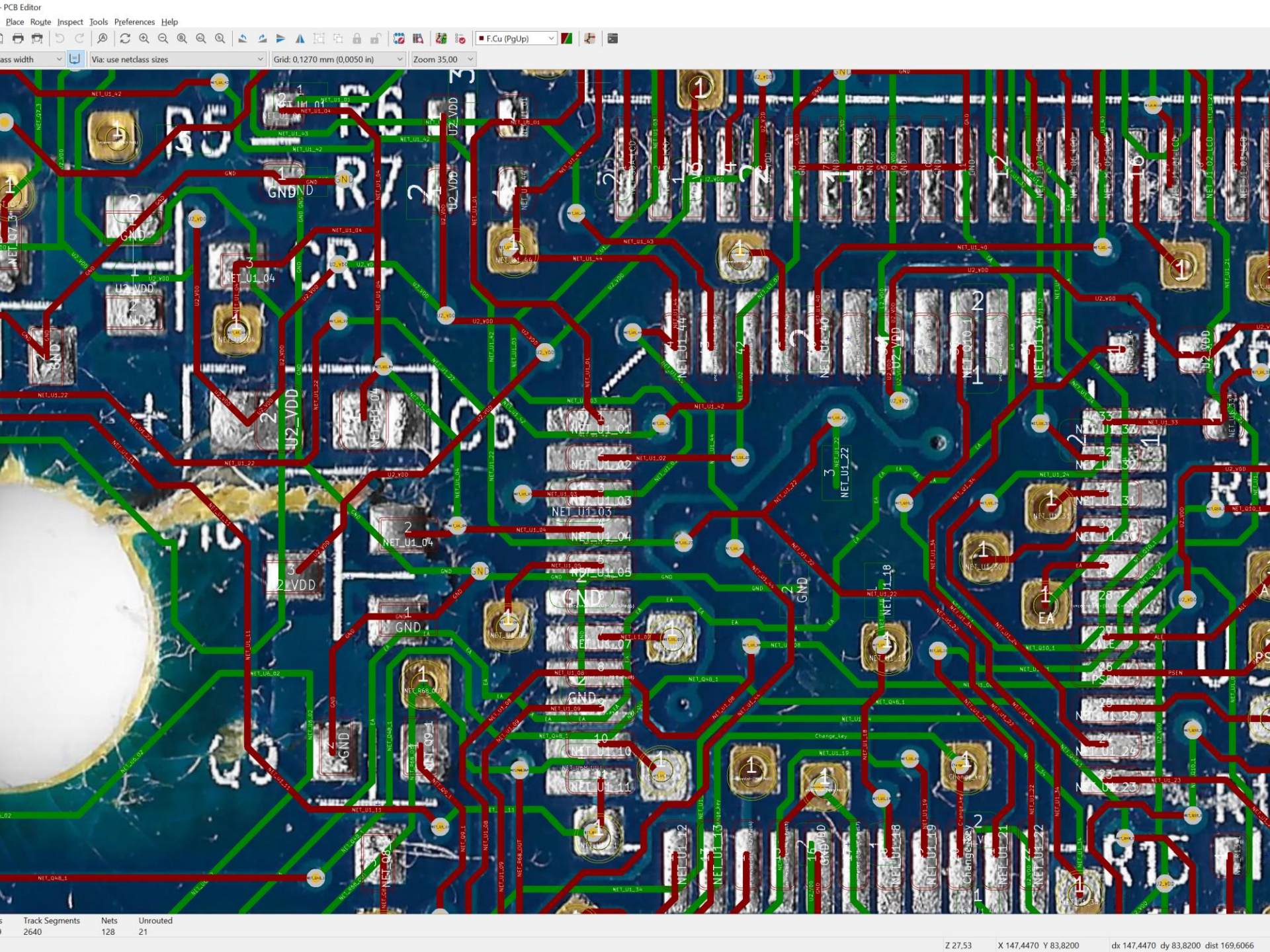
- Old components impossible to find
- Do I really need to go this deep?
- Spend ~1 month full time on the process

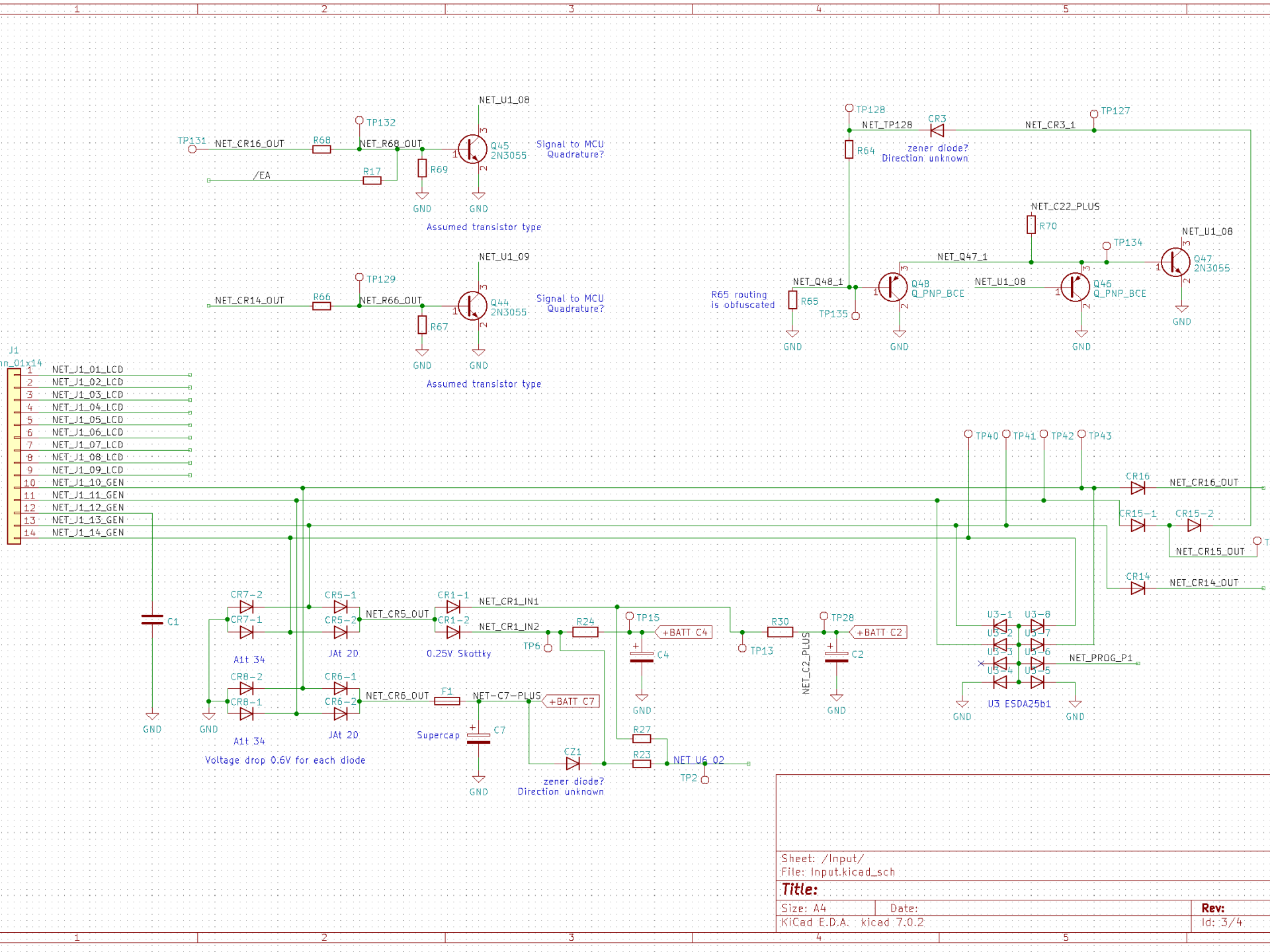

BAKU 858D
350
DIGITAL
SKYTRONIC

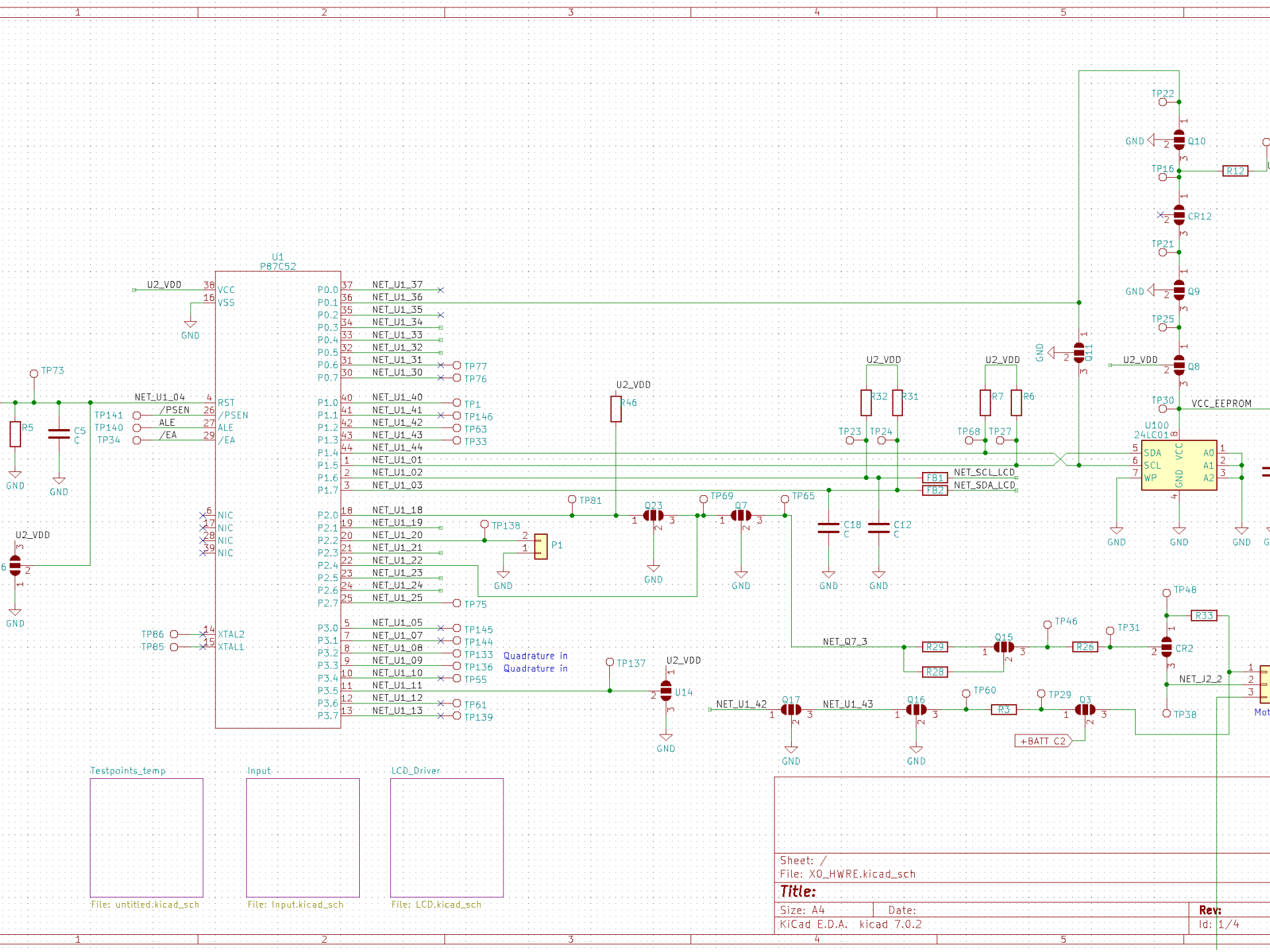
	1	2	3	4	5	6	7	8	9	10
A	F2	CR2	CR4	CR3	CR1	R23	R21	CR10	Q8	Q15
	Q17	Q18	CR9	CR8	R22				U6	U4
	Y1	C4 C13 C4 C18	U1	U8	U7	R14	CR7	CR6	Q2	Q3
							U5	U9	P1	RT1
	C16	FB1	R20	R19	C9	CR17	R39	R30	R38	C44 15
	Q4	R31	Q13	Q12	R17	Q10	Q15	Q14	FB2	C17
	Q9	R26	R18	Q16	R32	R13	R25	CR13	C3	R1
	R3	Q1	C12	R24	Q7	CR11	C21	R35	R36 2	C11




C2
JP1
CR16
CR14
R66
Q5
CZ1
CZ3
U1
U2
R67
F1
U4
R3
U3
JP2
U5
R1
U6
R5
R6
R7
U14
CR15
Q7
CR4
C6
R8
R10
R60
R9
C5
U8
U11
CR3
Q13
R20
Q9
R13
R15
R14
U10
Q34
R12
R17
C7
Q11
R65
Q45
503049
Rev C


PCB Editor
Place Route Inspect Tools Preferences Help
F.Cu (PgUp)
Via: use netclass sizes
Grid: 0,1270 mm (0,0050 in)
Zoom 35,00
U2_VDD
GND
NET_U1_01
NET_U1_02
NET_U1_03
NET_U1_04
NET_U1_05
NET_U1_10
NET_U1_11
NET_U1_12
NET_U1_13
NET_U1_18
NET_U1_19
NET_U1_21
NET_U1_22
NET_U1_23
NET_U1_24
NET_U1_25
NET_U1_30
NET_U1_31
NET_U1_32
NET_U1_33
NET_U1_34
NET_U1_40
NET_U1_42
NET_U1_43
NET_U1_44
EA
PSEN
ALE
Change_key
Track Segments
2640
Nets
128
Unrouted
21
Z 27,53
X 147,4470 Y 83,8200
dx 147,4470 dy 83,8200 dist 169,6066

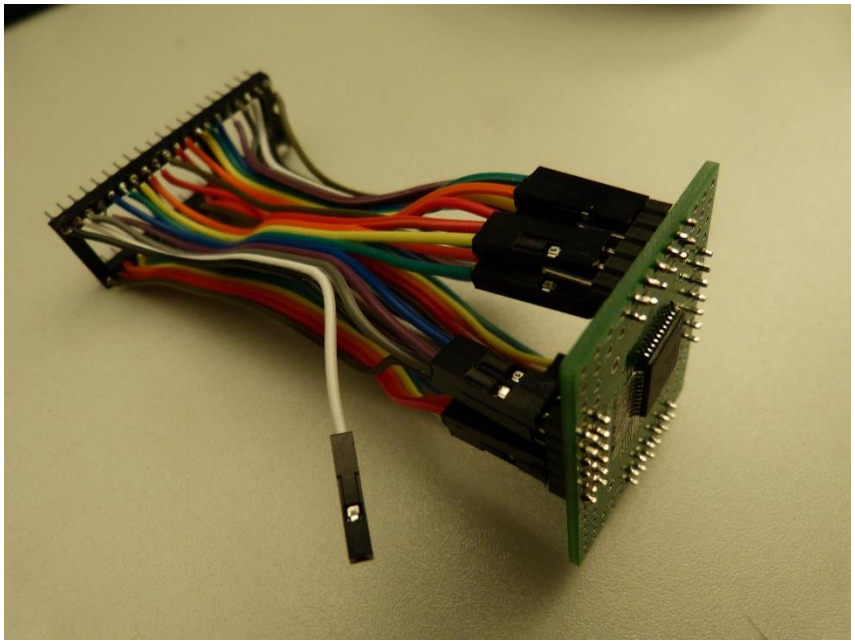

NET_U1_08
TP132
TP131
NET_CR16_OUT
R68
NET_R68_OUT
Q45
2N3055
Signal to MCU
Quadrature?
/EA
R17
R69
GND
GND
Assumed transistor type
NET_U1_09
TP129
NET_CR14_OUT
R66
NET_R66_OUT
Q44
2N3055
Signal to MCU
Quadrature?
R67
GND
GND
Assumed transistor type
TP128
NET_TP128
CR3
NET_CR3_1
TP127
R64
zener diode?
Direction unknown
NET_C22_PLUS
R70
TP134
NET_U1_08
NET_Q47_1
Q47
2N3055
NET_Q48_1
NET_U1_08
R65 routing
is obfuscated
R65
TP135
Q48
Q_PNP_BCE
Q46
Q_PNP_BCE
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
GND
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
GND
R30
TP13
TP28
+BATT C2
C2
GND
NET_C2_PLUS
U3-1
U3-2
U3-3
U3-4
U3-8
U3-7
U3-6
U3-5
NET_PROG_P1
U3 ESDA25b1
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
GND
Voltage drop 0,6V for each diode
CZ1
zener diode?
Direction unknown
R27
R23
NET_U6_02
TP2
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
TP75
TP145
TP144
TP133
TP136
TP55
TP61
TP139
Quadrature in
Quadrature in
TP138
P1
TP81
TP69
TP65
Q23
Q7
C18
C12
R46
U2_VDD
TP137
U14
R32
R31
R7
R6
TP23
TP24
TP68
TP27
FB1
FB2
NET_SCL_LCD
NET_SDA_LCD
TP22
Q10
R12
TP16
CR12
TP21
Q9
TP25
Q11
Q8
TP30
VCC_EEPROM
U100
24LC01
SDA
SCL
WP
VCC
A0
A1
A2
TP48
R33
TP46
TP31
R29
R28
Q15
R26
CR2
NET_Q7_3
NET_J2_2
TP38
NET_U1_42
NET_U1_43
Q17
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

- Locked & fused & encrypted
- Xgcu Tl866II Programmer with Xgpro
  - Changed to Minipro (CLI)
- Listen with a logic analyzer

- 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

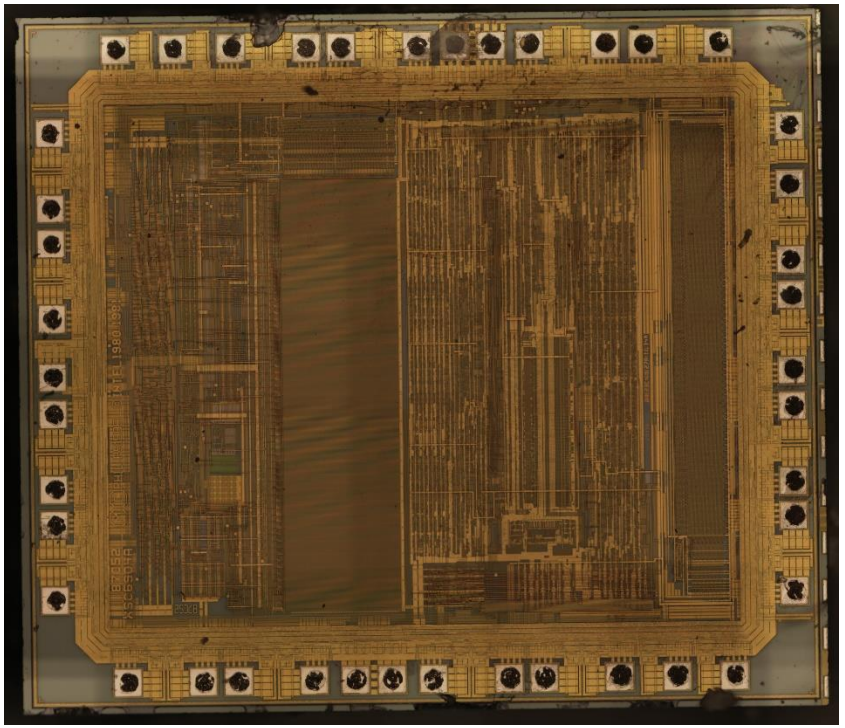
Default Programmer(1): TL866II-Plus

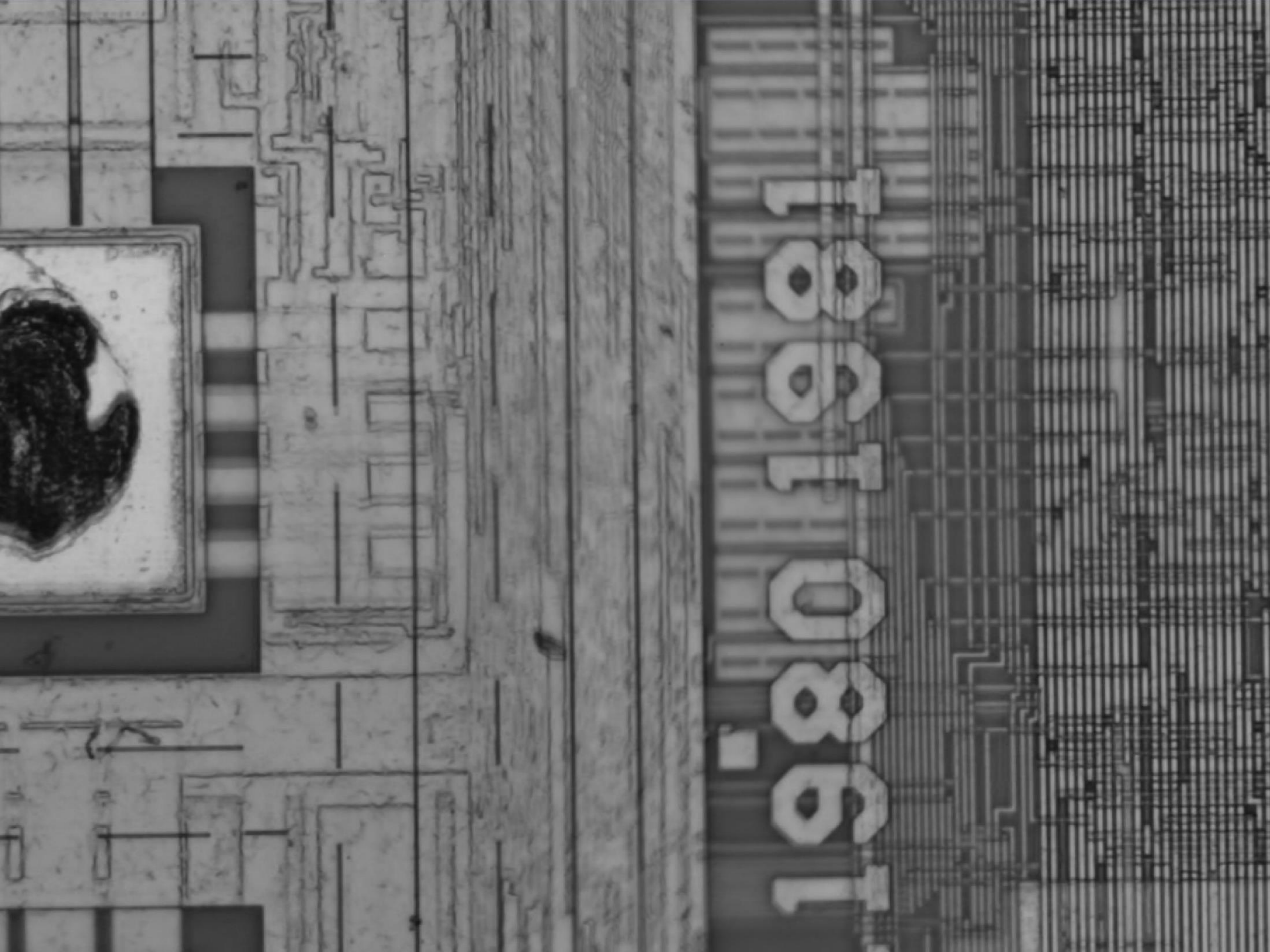
0000 0000

Chip reverse engineering

riscure

- Decap many chips
  - Heat & twist
- Polishing
- Photographing
  - Metallurgical microscope
  - Stitching – 208MP
- Other
  - Micro probing
  - SEM from friends
  - International collaboration




1980 1981

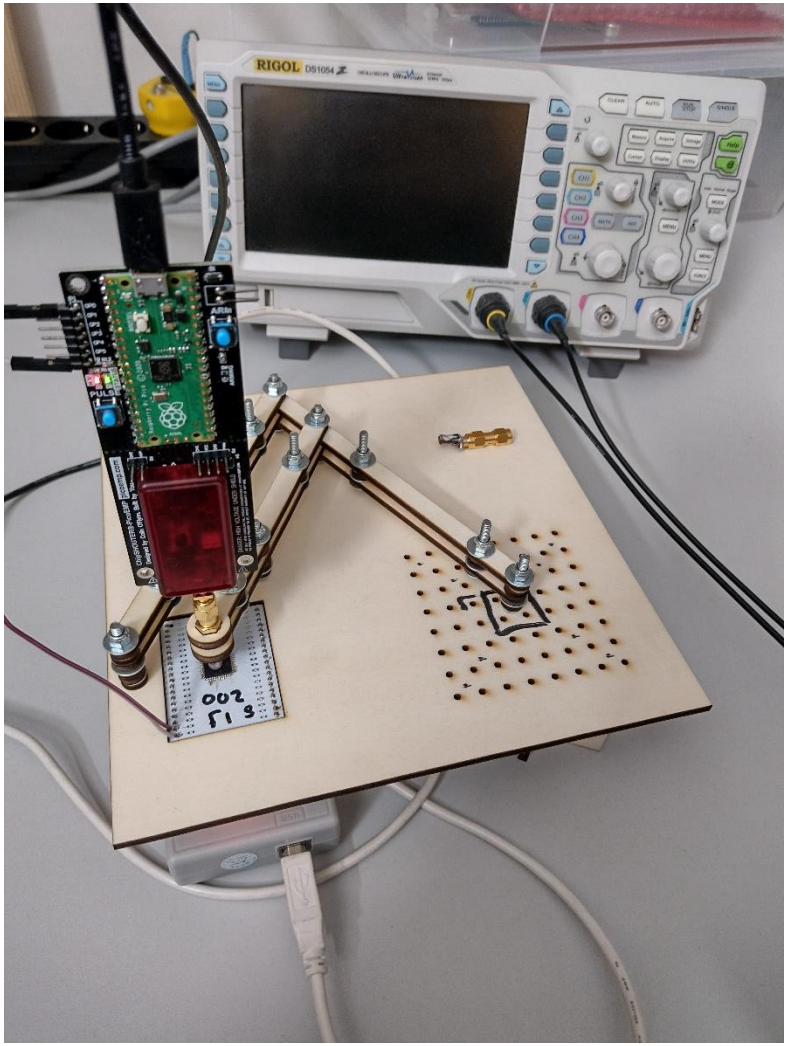
Fault injection

riscure

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

Fault injection

- PicoEMP
  - DIY
  - Opensource
  - € 100 in parts
  - Slightly underpowered
- Human XYZ
  - Pantograph



Fault injection

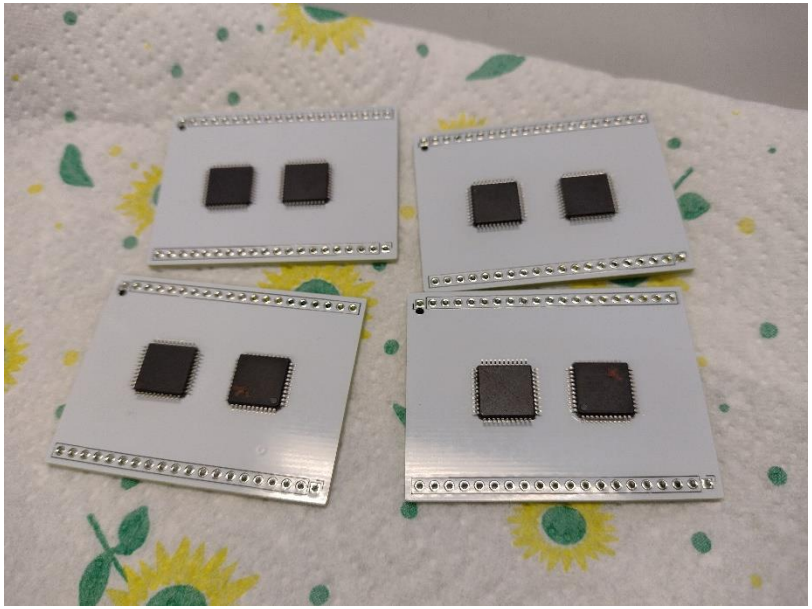
riscure

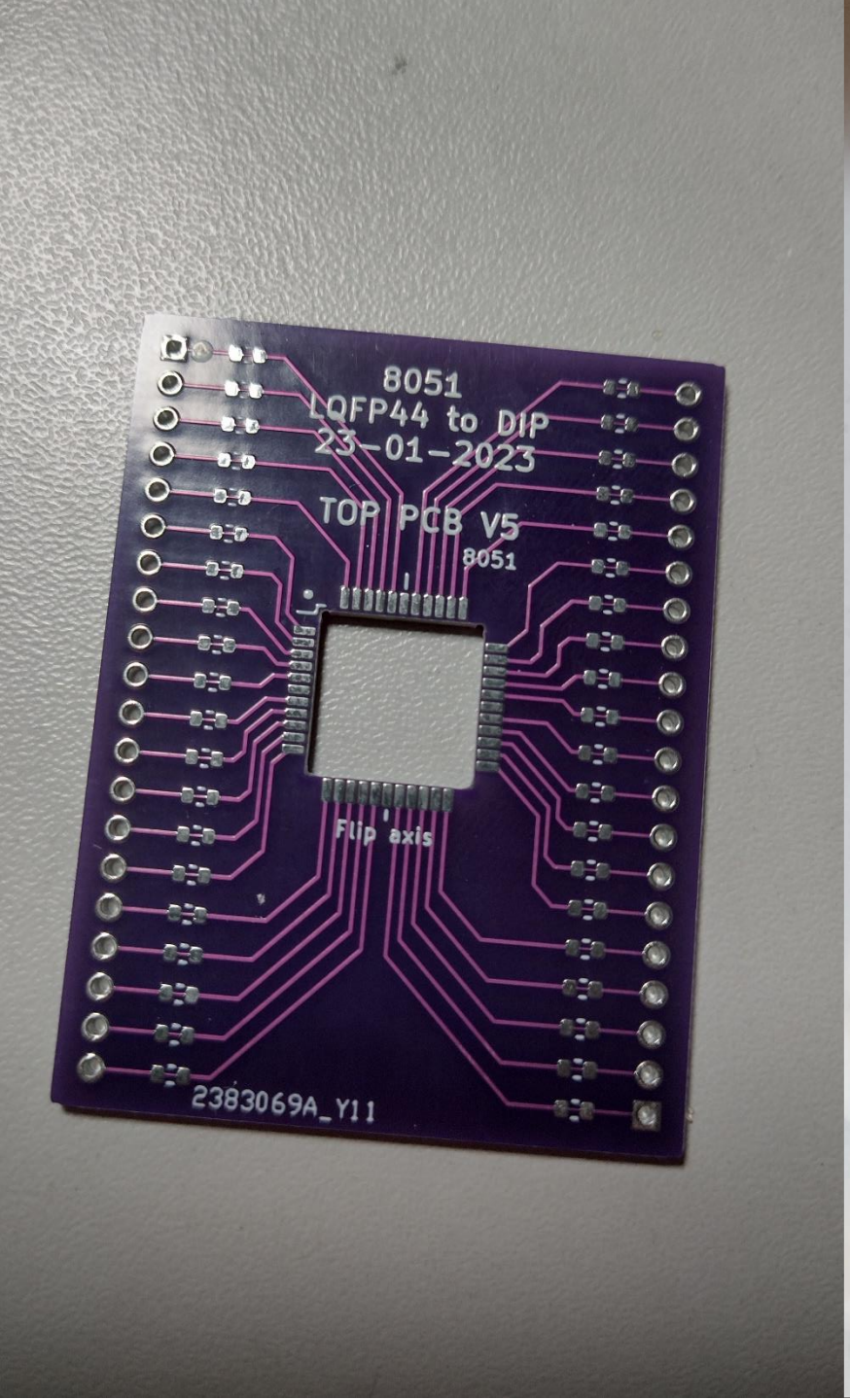
- Human XYZ

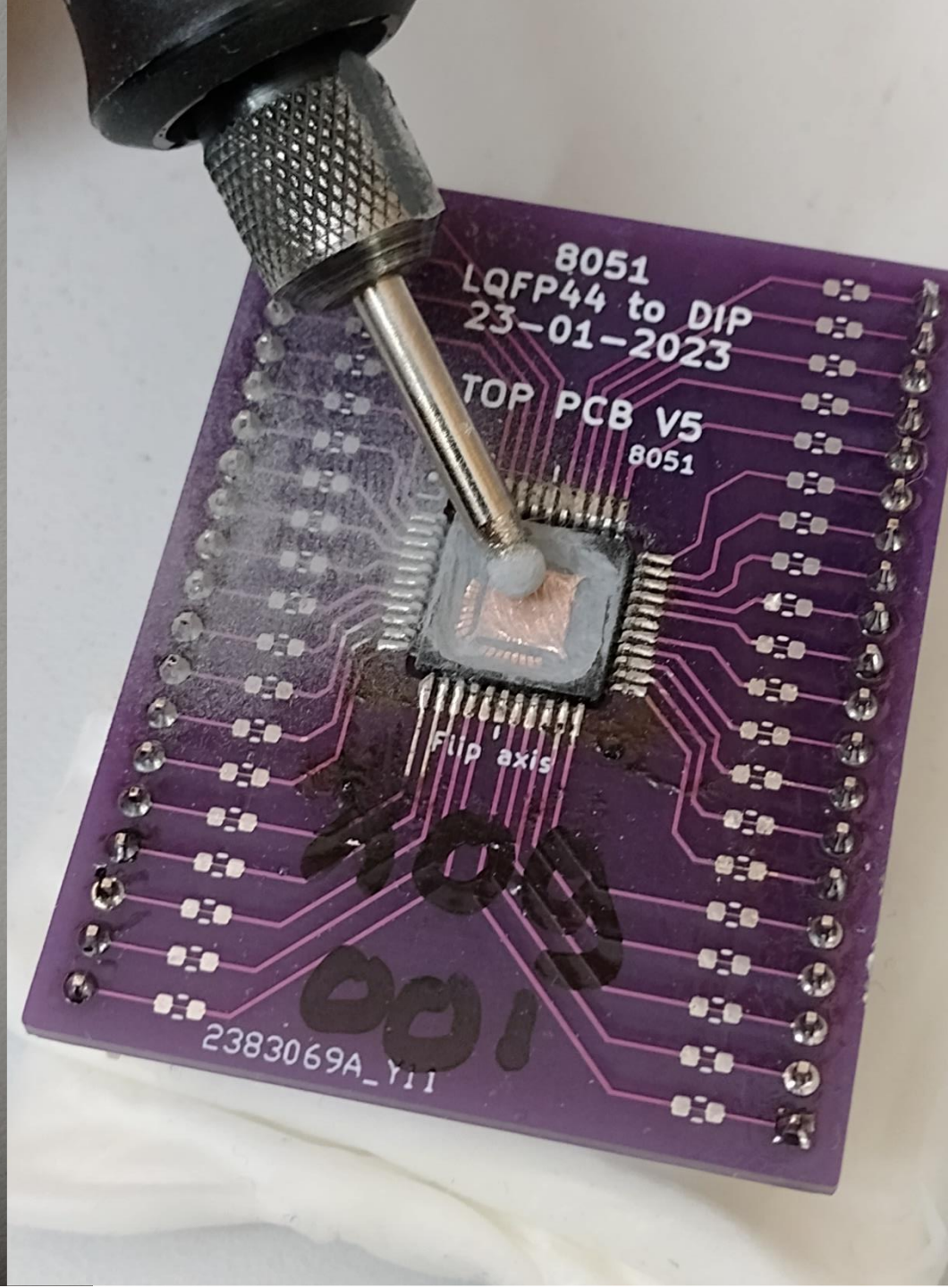
```
1
2  # define grid
3
4  x = 0
5  y = 1
6  top_left = [3,3]
7  bottom_right = [6,6]
8  scaler = 1
9
10 for x_coordinate in range(top_left[x]*scaler, bottom_right[x] *scaler+1):
11     for y_coordinate in range(top_left[y]*scaler, bottom_right[y]*scaler+1):
12         print(f'Hello Human, please move me to coordinates: [{x_coordinate},{y_coordinate}]')
13         input()
14         print('Thank you.')
15
16
```

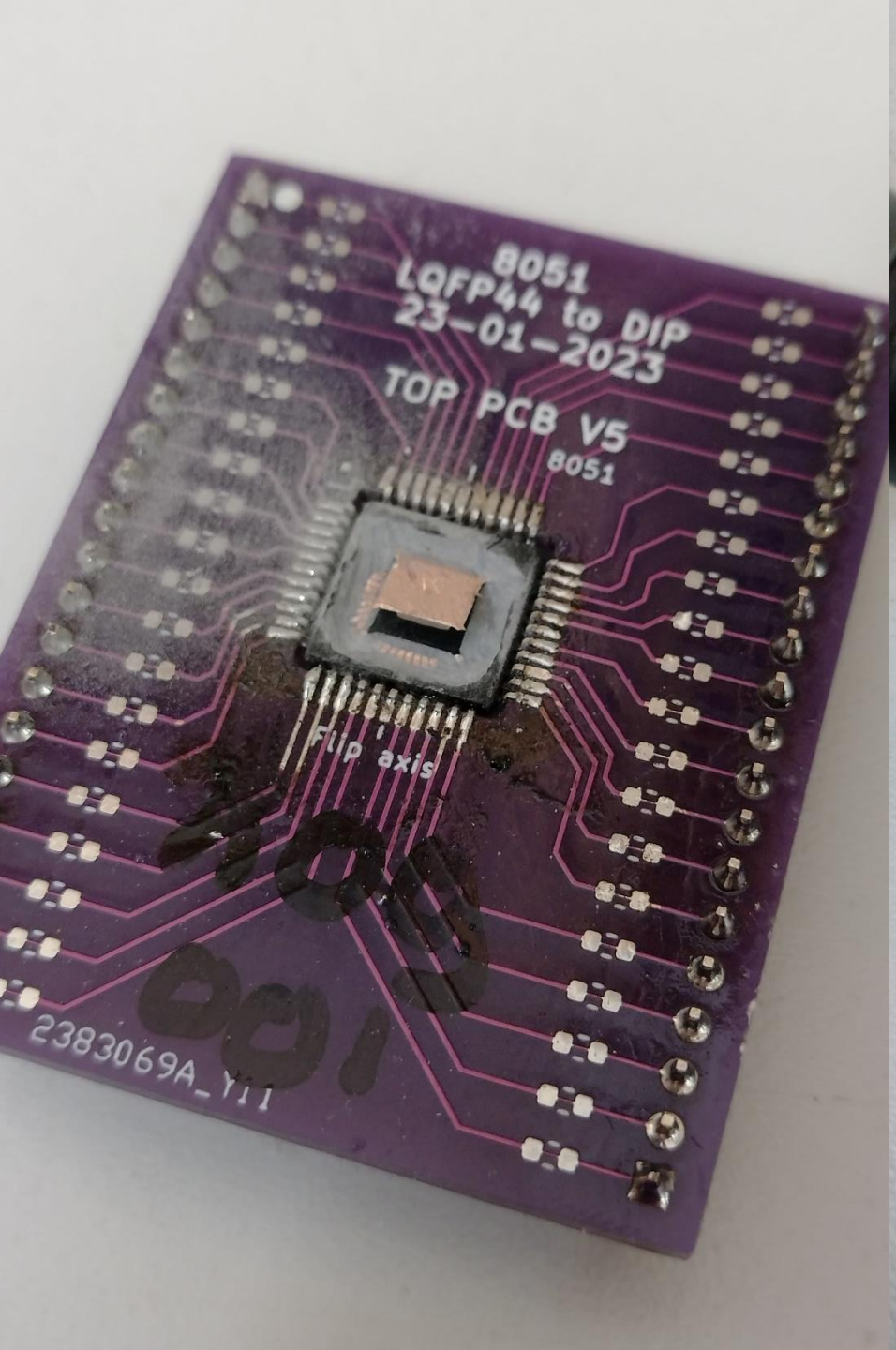
Fault injection

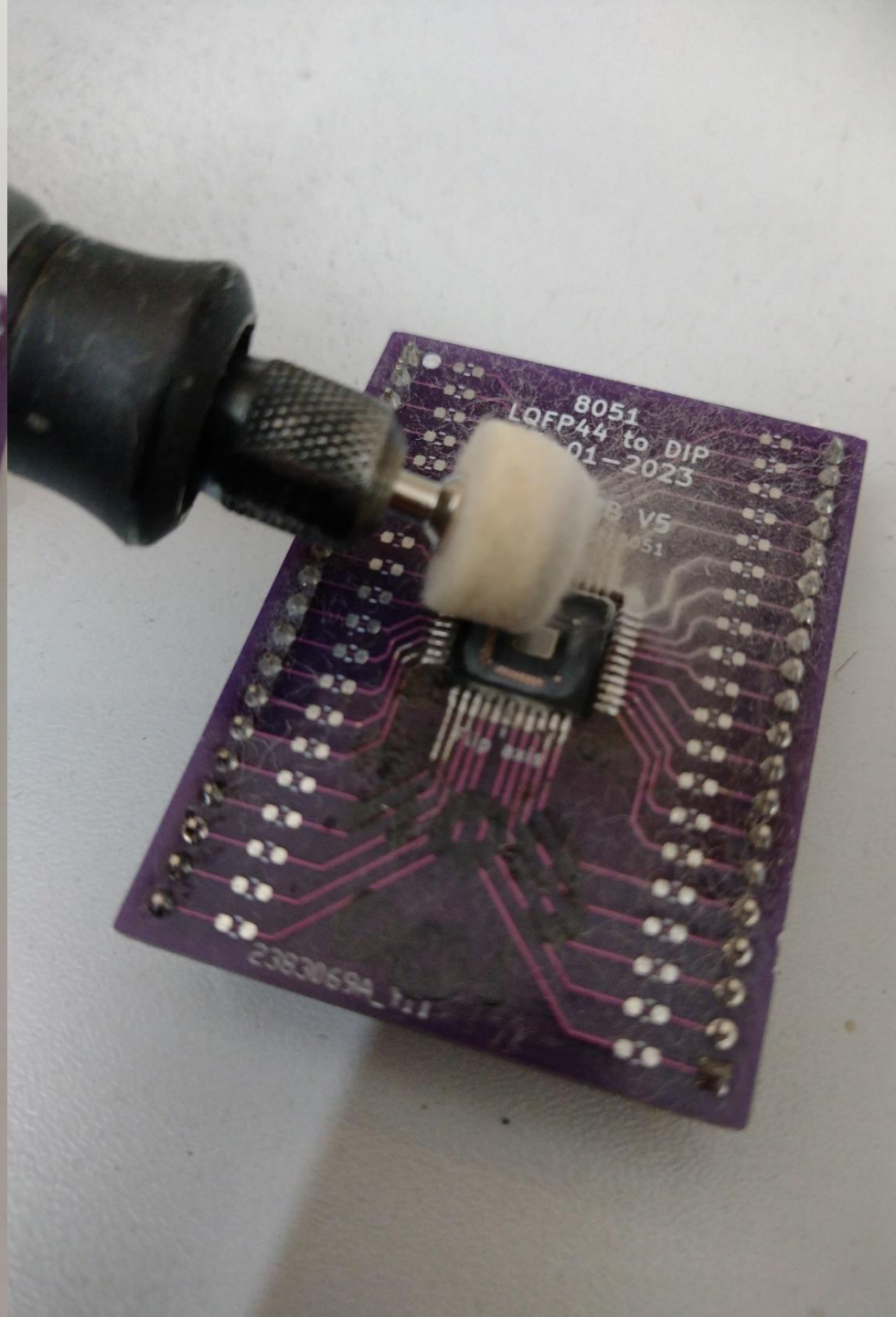
- Sample preparation for Laser FI
  - Milling
    - Proxxon
    - Learning curve
    - Little feedback
  - Dremel
    - Quick and reliable
    - Needed a new adapter
  - Multiple chip versions

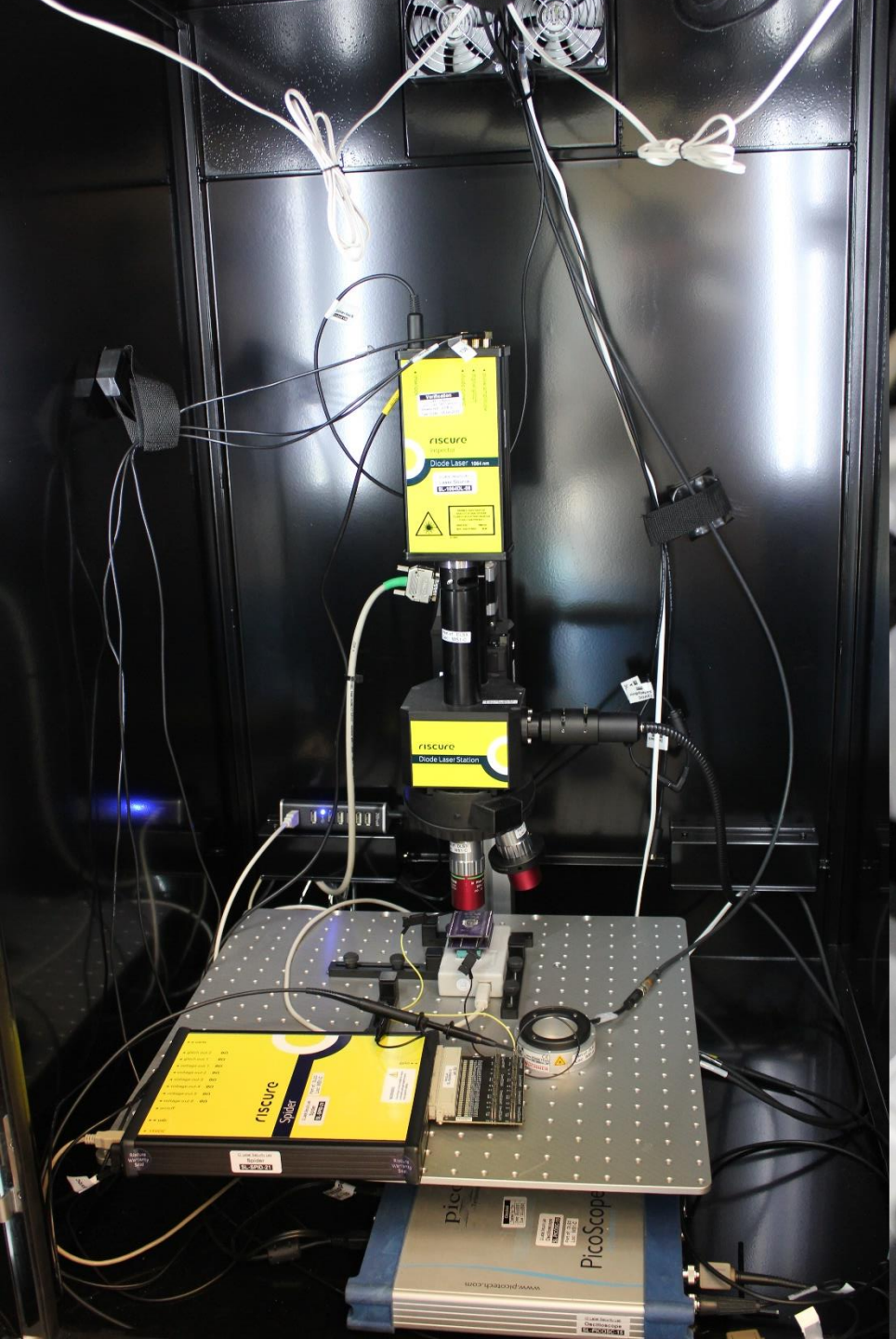


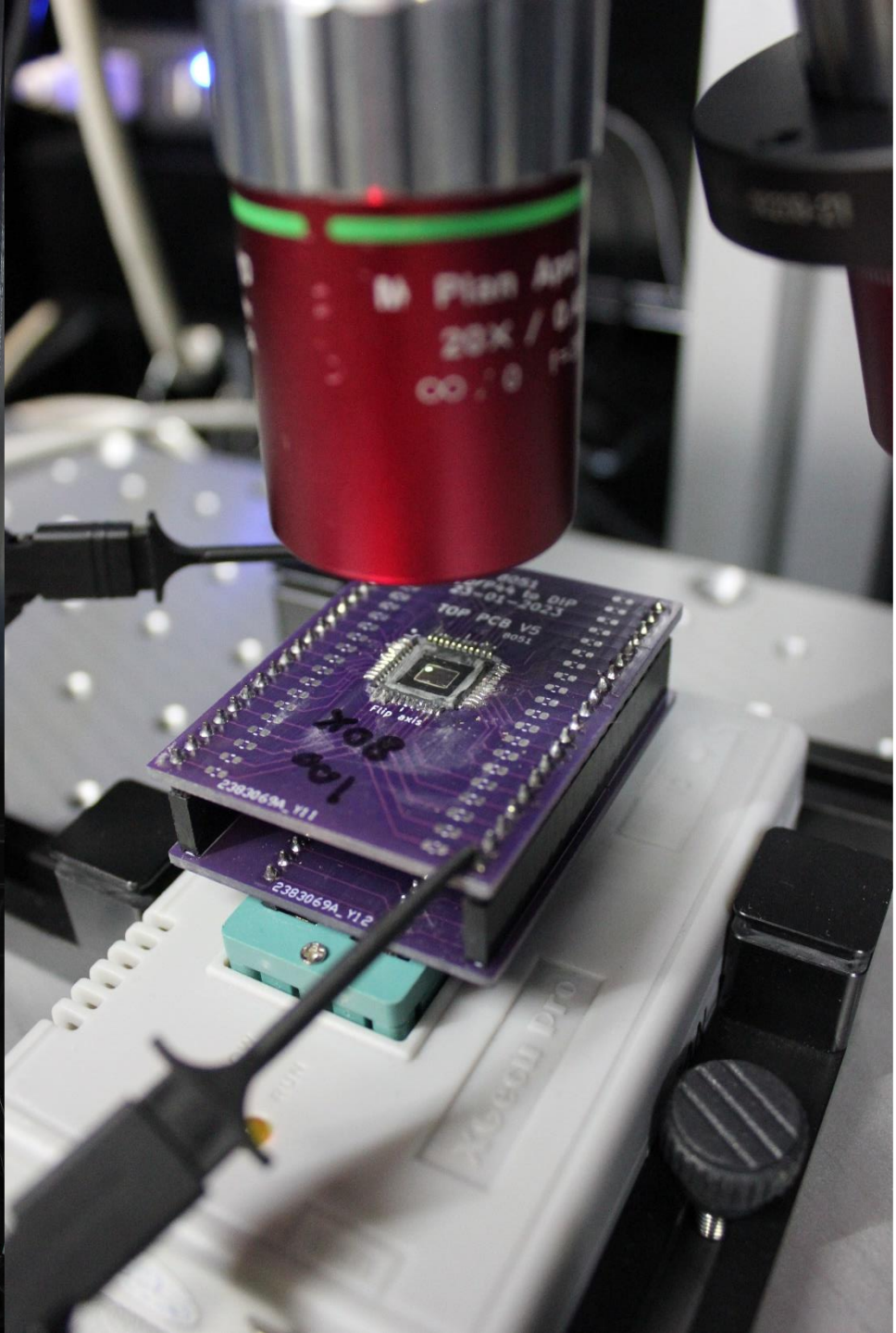

8051
LQFP44 to DIP
23-01-2023
TOP PCB V5
8051
Flip axis
2383069A_Y11

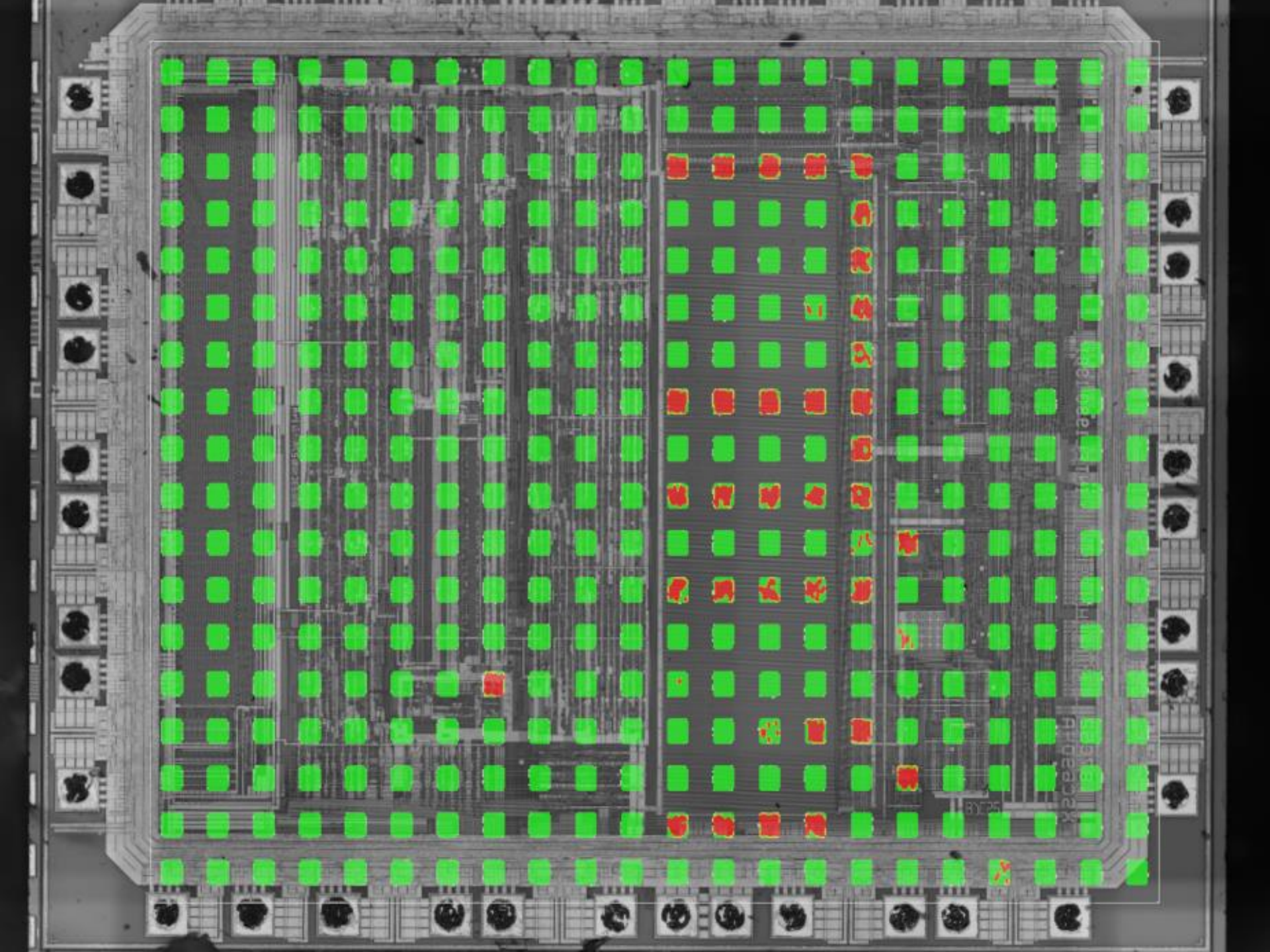

8051
LQFP44 to DIP
23-01-2023
TOP PCB V5
8051
Flip axis
2383069A_Y11

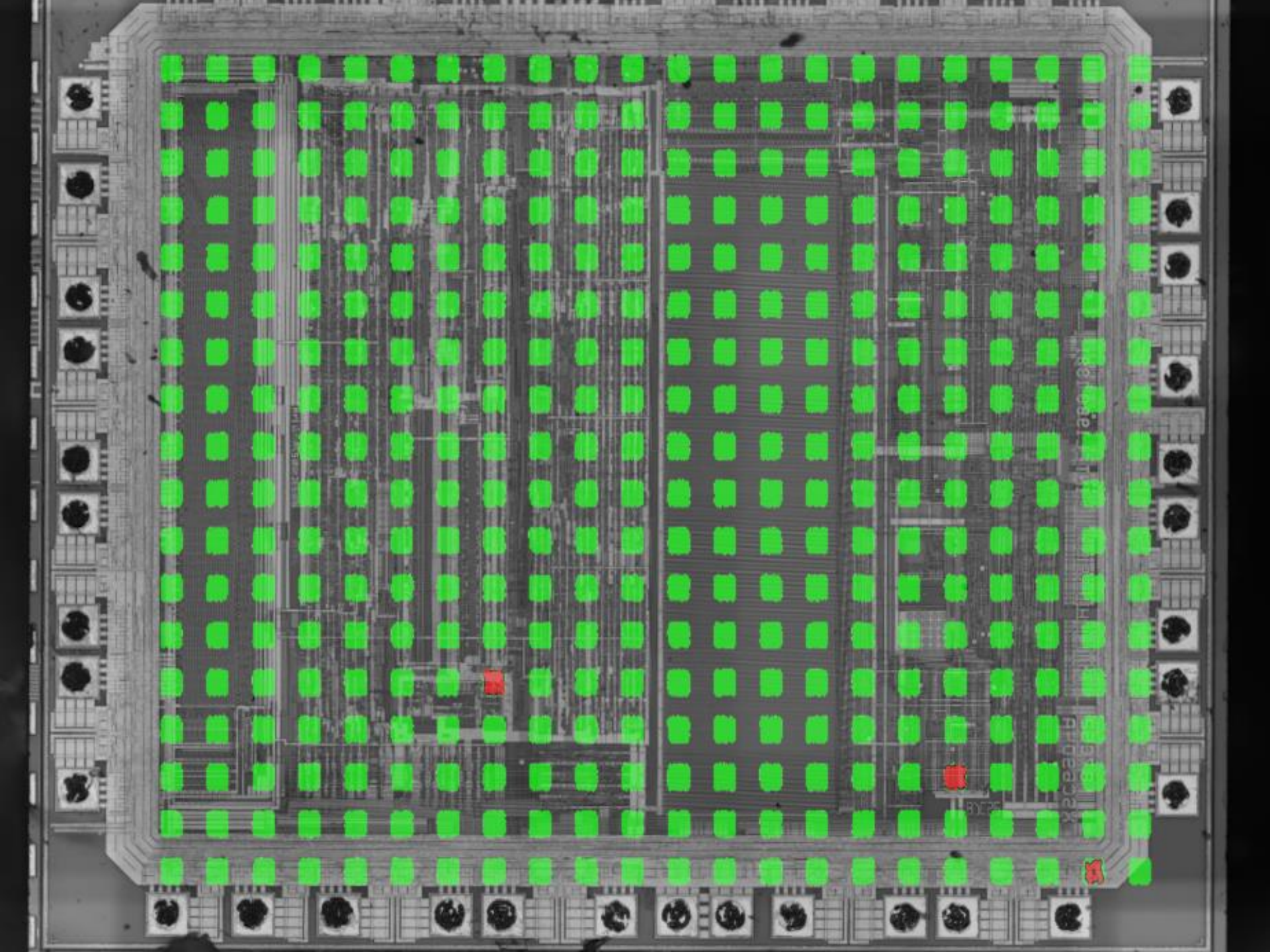

8051
LQFP44 to DIP
23-01-2023
TOP PCB V5
8051
Flip axis
2383069A_Y11


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

Process

- One month in off hours

- X07
  - Successful
  - Failed to dump 2nd chip
- X08
  - Successful
- X09
  - Successfully dumped multiple versions

Laser = Success

riscure

"Encryption"

- XOR table
  - More difficult than expected

Attacks

- Repeating content
- Known content -> Factory defaults
- ASCII -> Copyright notice
- Partial unencrypted -> 64 / 128 byte blocks

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

Future work

- Learn 8051 architecture
- Learn Software reverse engineering
- Try a more ‘Abrasive’ method