Multiplexed Wired Attack Surfaces

Michael Ossmann
@michaelossmann

Kyle Osborn
@thekos

Black Hat USA 2013

You've locked
your Android
device.

You've disabled debugging (adb).

A customs officer can still plug into your USB port and get a shell.

XDA Developers

public knowledge

not common knowledge

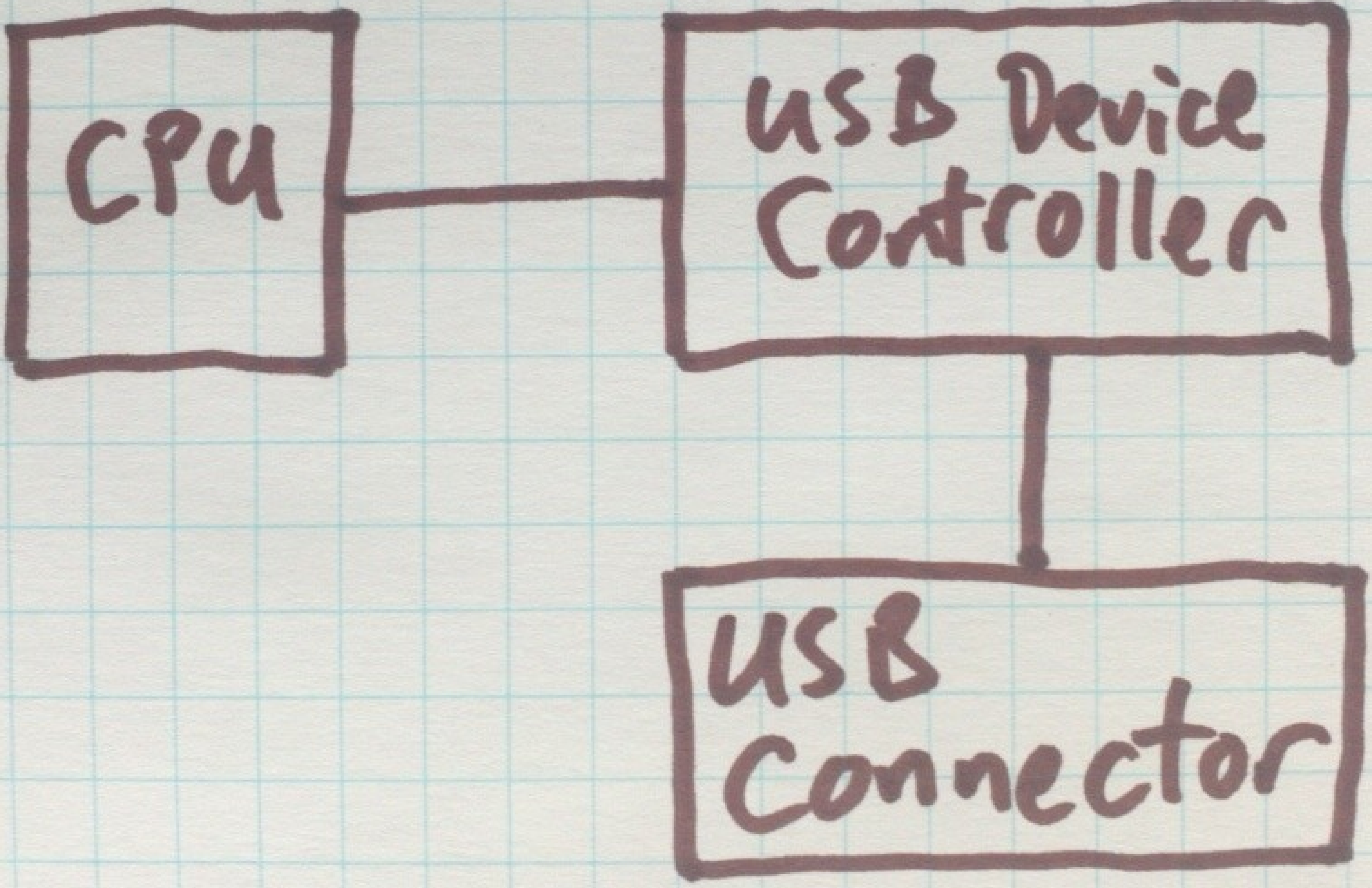
Connectors and Cables repurposed

PoE

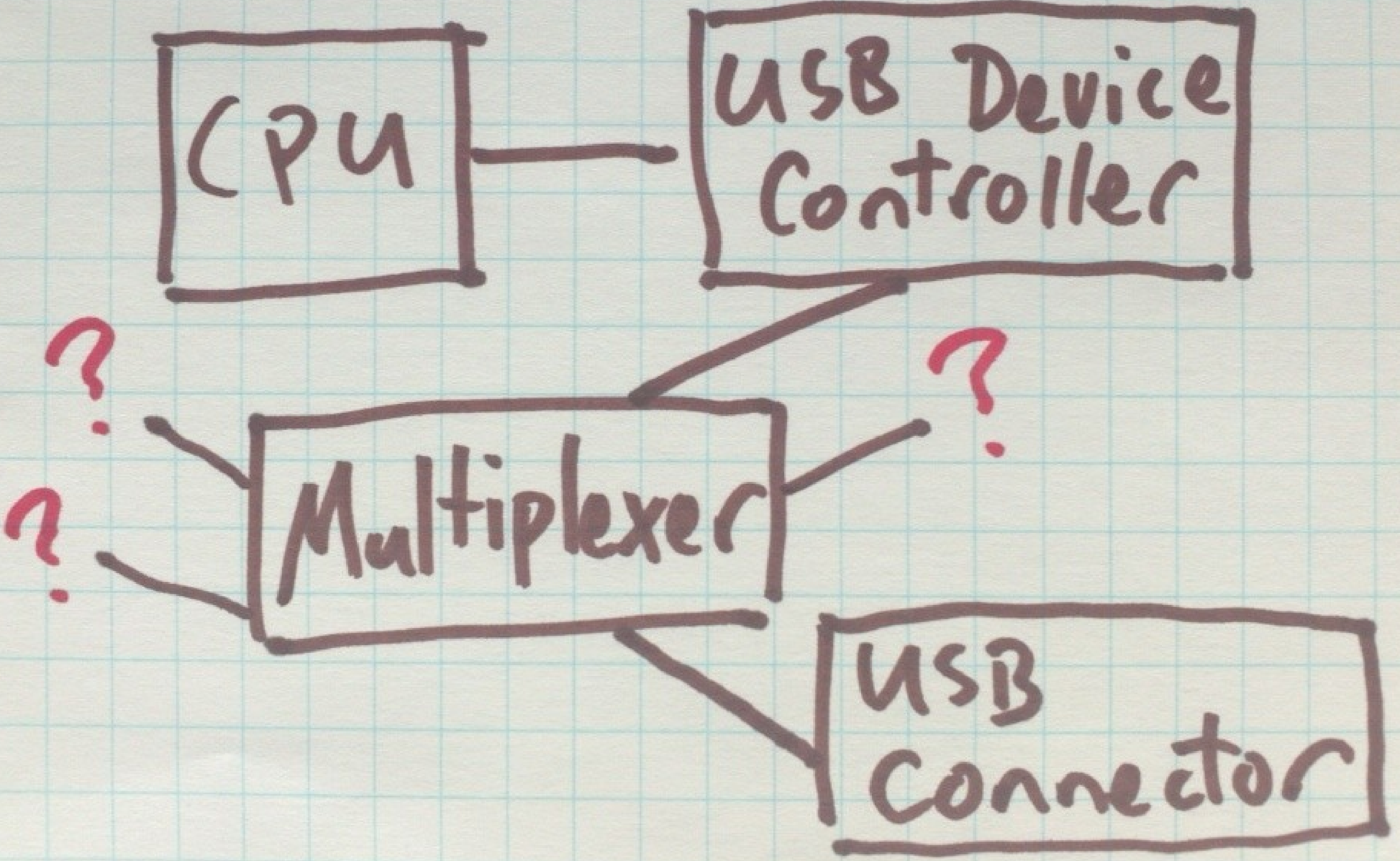
DSL

iPod shuffle

A Typical USB Device



A Mobile Phone



Multiplexed Functions

USB On-the-Go (OTG)

Audio (USB Car kit)

Debug and Programming Interfaces

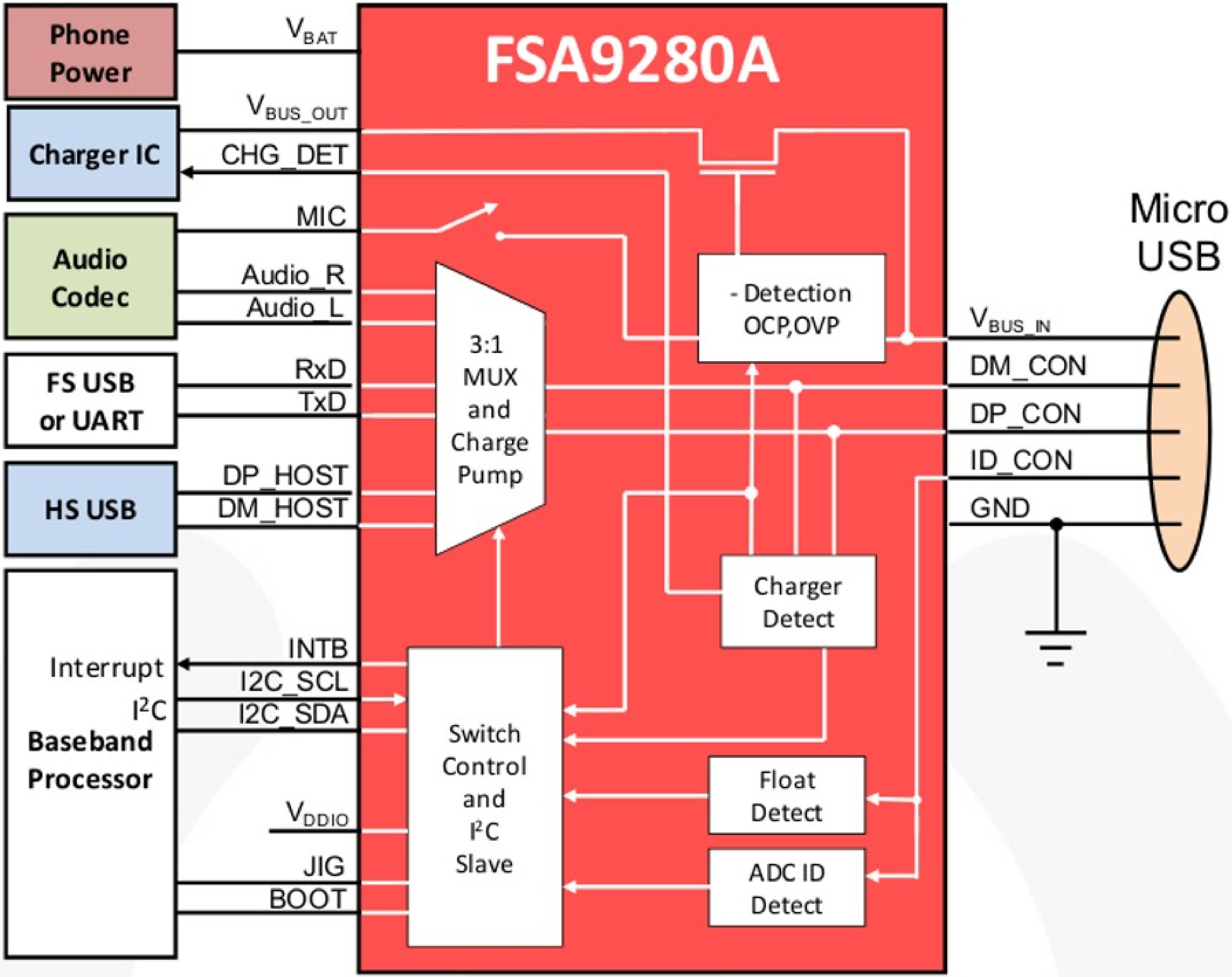
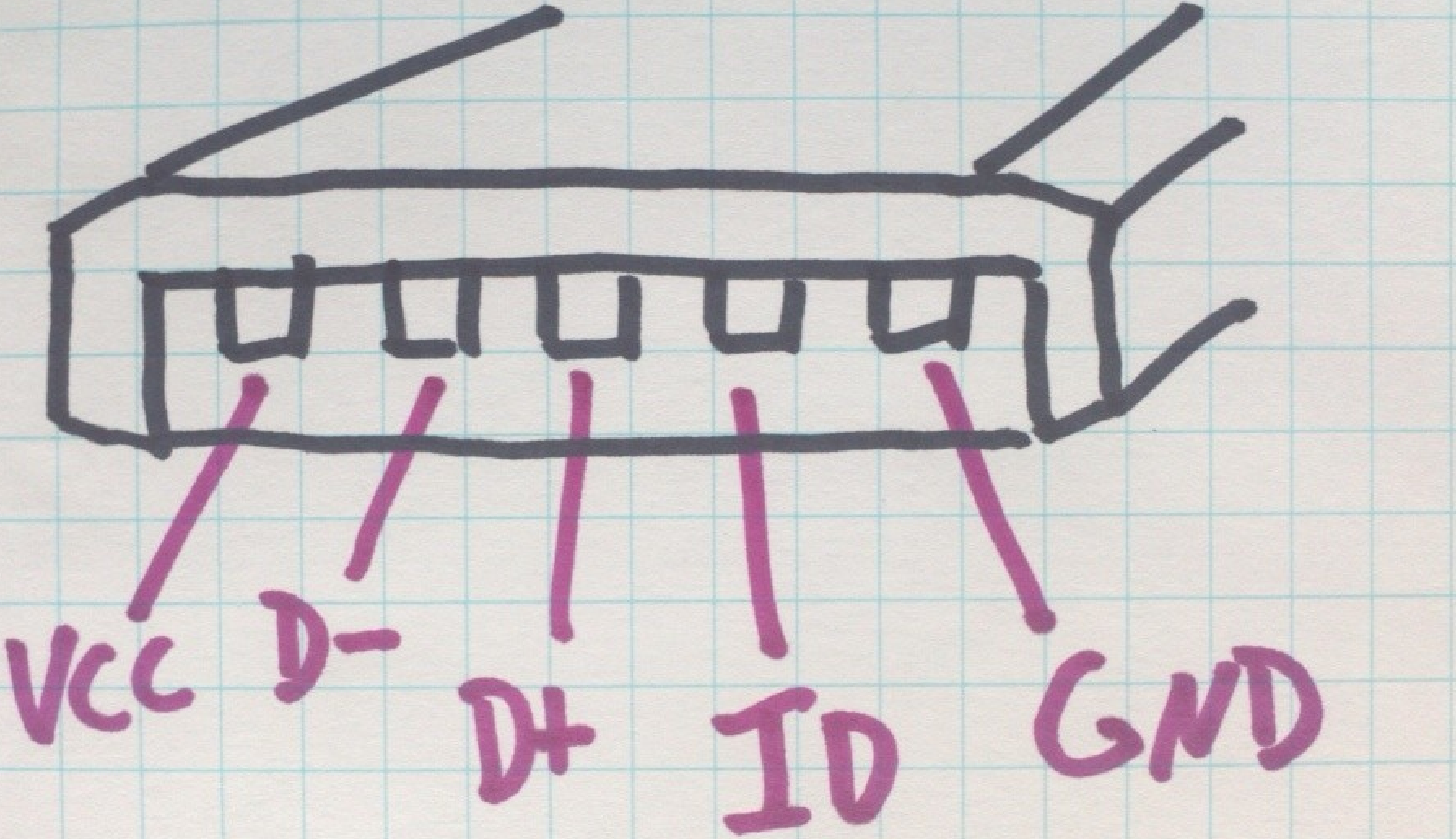


Figure 2. Block Diagram


VCC
D-
D+
ID
GND

Binary Value[4]	ID_CON resistance to GND			Accessory Detected[5]
	Min.	Typ.	Max.	
00000	GND	GND	GND	DO NOT USE
00001	1.9kΩ	2kΩ	2.1kΩ	Audio Send/End Button
00010	2.47kΩ	2.604kΩ	2.73kΩ	Audio Remote S1 Button[6]
00011	3.05kΩ	3.208kΩ	3.37kΩ	Audio Remote S2 Button[6]
00100	3.81kΩ	4.014kΩ	4.21kΩ	Audio Remote S3 Button[6]
00101	4.58kΩ	4.82kΩ	5.06kΩ	Audio Remote S4 Button[6]
00110	5.73kΩ	6.03kΩ	6.33kΩ	Audio Remote S5 Button[6]
00111	7.63kΩ	8.03kΩ	8.43kΩ	Audio Remote S6 Button[6]
01000	9.53kΩ	10.03kΩ	10.53kΩ	Audio Remote S7 Button[6]
01001	11.43kΩ	12.03kΩ	12.63kΩ	Audio Remote S8 Button[6]
01010	13.74kΩ	14.46kΩ	15.18kΩ	Audio Remote S9 Button[6]
01011	16.4kΩ	17.26kΩ	18.12kΩ	Audio Remote S10 Button[6]
01100	19.48kΩ	20.5kΩ	21.53kΩ	Audio Remote S11 Button[6]
01101	22.87kΩ	24.07kΩ	25.27kΩ	Audio Remote S12 Button[6]
01110	27.27kΩ	28.7kΩ	30.14kΩ	Reserved Accessory #1
01111	32.3kΩ	34kΩ	35.7kΩ	Reserved Accessory #2
10000	38.19kΩ	40.2kΩ	42.21kΩ	Reserved Accessory #3
10001	47.41kΩ	49.9kΩ	52.4 kΩ	Reserved Accessory #4
10010	61.66kΩ	64.9kΩ	68.15kΩ	Reserved Accessory #5
10011	76.1kΩ	80.7kΩ	84.1kΩ	DO NOT USE
10100	96.9kΩ	102kΩ	107.1kΩ	DO NOT USE
10101	115kΩ	121kΩ	127kΩ	TTY Converter
10110	143kΩ	150kΩ	157kΩ	UART Cable
10111	190kΩ	200kΩ	210kΩ	*See Table 4*
11000	242kΩ	255kΩ	268kΩ	Factory Mode Boot OFF-USB[7]
11001	292kΩ	301kΩ	316kΩ	Factory Mode Boot ON-USB[7]
11010	347kΩ	365kΩ	383kΩ	DO NOT USE
11011	419.9kΩ	442kΩ	464kΩ	*See Table 4*
11100	507kΩ	523kΩ	549kΩ	Factory Mode Boot OFF-UART[7]
11101	588kΩ	619kΩ	650kΩ	Factory Mode Boot ON-UART[7]
11110	750kΩ	1000kΩ	1050kΩ	Audio Type 1 with Remote[8]
	750kΩ	1002kΩ	1050kΩ	Audio Type 1 / Only Send-End[8]

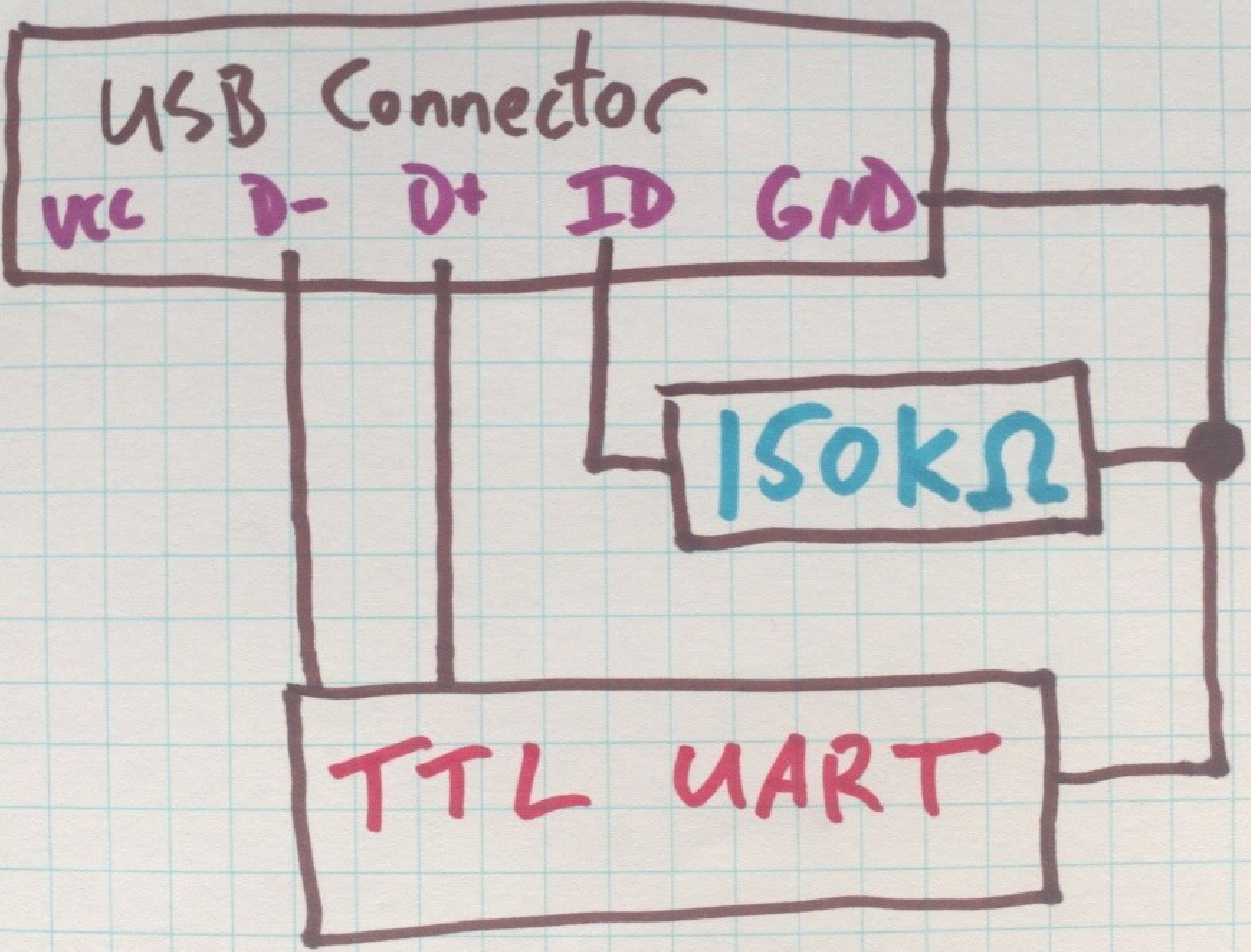
64.9kΩ	68.15kΩ	Reserved Accessory #5
80.7kΩ	84.1kΩ	DO NOT USE
102kΩ	107.1kΩ	DO NOT USE
121kΩ	127kΩ	TTY Converter
150kΩ	157kΩ	UART Cable
200kΩ	210kΩ	*See Table 4*
255kΩ	268kΩ	Factory Mode Boot OFF-USB[7]
301kΩ	316kΩ	Factory Mode Boot ON-USB[7]
365kΩ	383kΩ	DO NOT USE
442kΩ	464kΩ	*See Table 4*
523kΩ	549kΩ	Factory Mode Boot OFF-UART[7]
619kΩ	650kΩ	Factory Mode Boot ON-UART[7]
1000kΩ	1050kΩ	Audio Type 1 with Remote[8]
1000kΩ	1050kΩ	Audio Type 1 / Only Send End[8]

UART

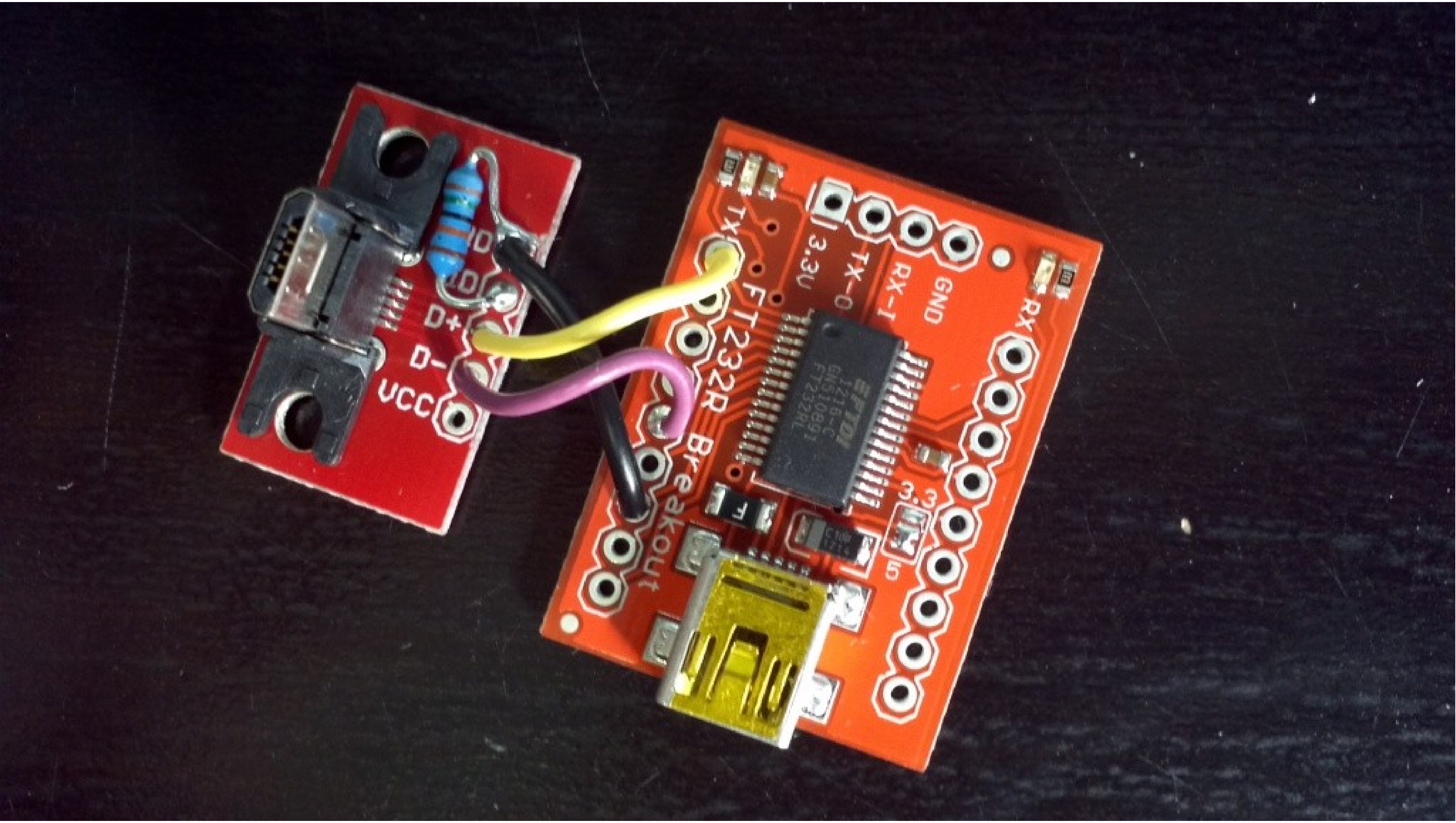
9600
19200
38400
115200
etc.

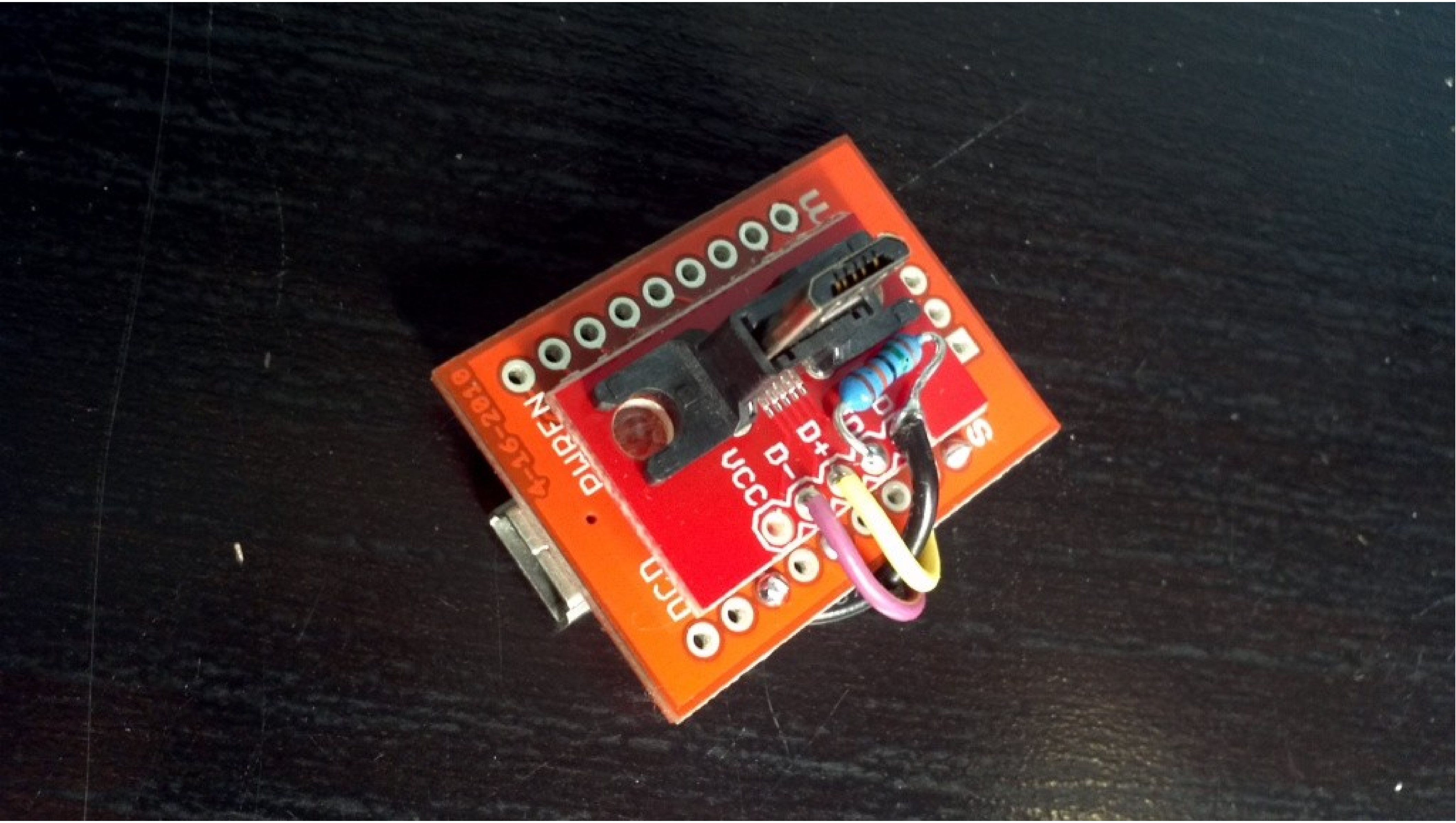
RS-232: crazy +/- V

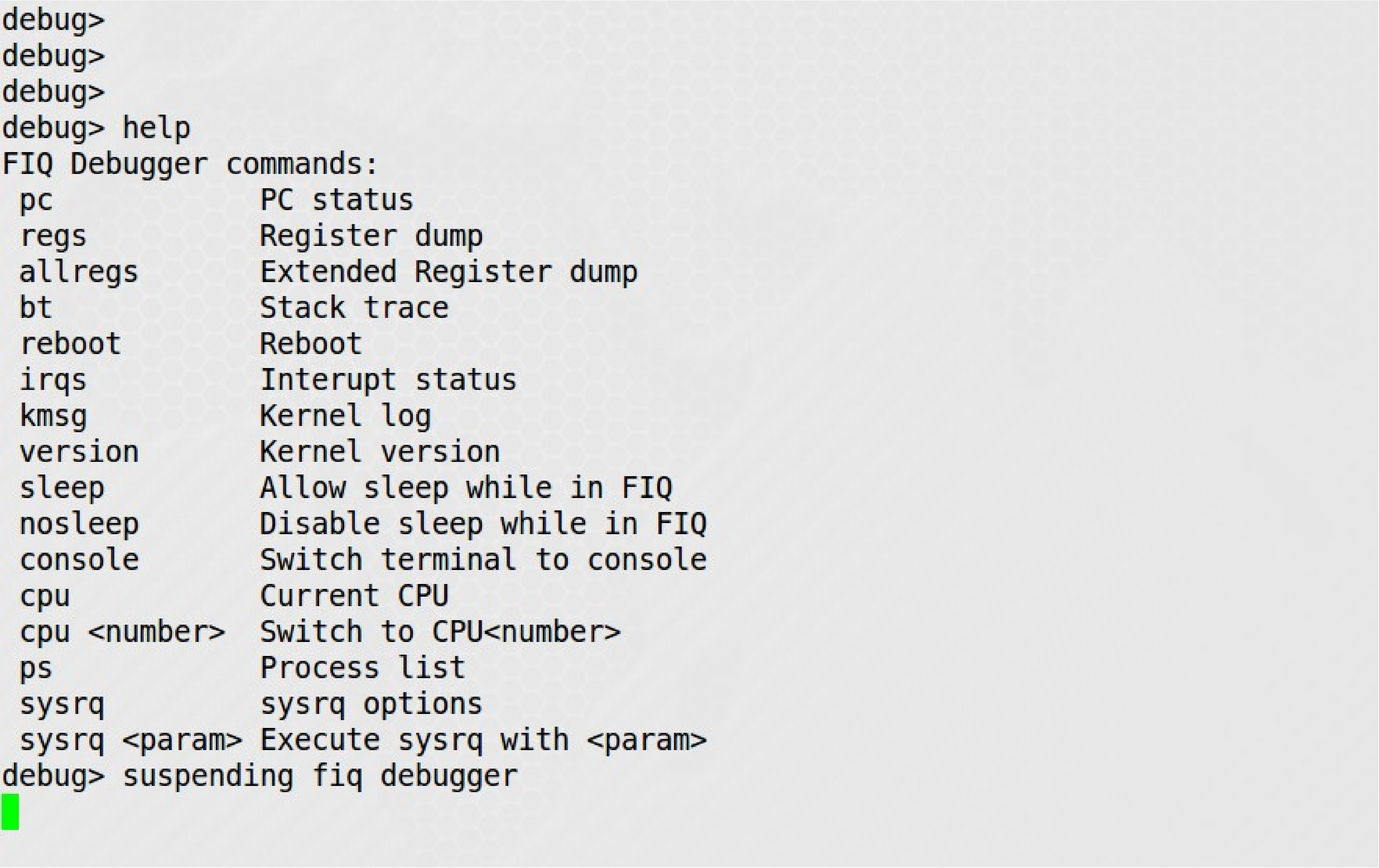
TTL: 0 to low V


USB Connector
VCC
D-
D+
ID
GND
150kΩ
TTL UART

Let's build it!


D+
D-
VCC
TX
3.3V
TX-O
RX-I
GND
RX
FT232R Breakout
3.3
5
F
FTDI
FT232RL


4-16-2010
D+
D-
VCC



```
debug>
debug>
debug>
debug> help
FIQ Debugger commands:
 pc            PC status
 regs          Register dump
 allregs       Extended Register dump
 bt            Stack trace
 reboot        Reboot
 irqs          Interupt status
 kmsg          Kernel log
 version       Kernel version
 sleep         Allow sleep while in FIQ
 nosleep       Disable sleep while in FIQ
 console       Switch terminal to console
 cpu           Current CPU
 cpu <number>  Switch to CPU<number>
 ps            Process list
 sysrq         sysrq options
 sysrq <param> Execute sysrq with <param>
debug> suspending fiq debugger
```

FIQ Debugger

arch/arm/common/fiq_debugger.c

pc　　bt　　kgdb*

allregs　　console

*usually compiled in read-only unprivileged mode without kgdb

FIQ Debugger

detailed process information

registers in use

kernel log

kernel debugger

console shell

Let's try it!

Commercial Test Jigs

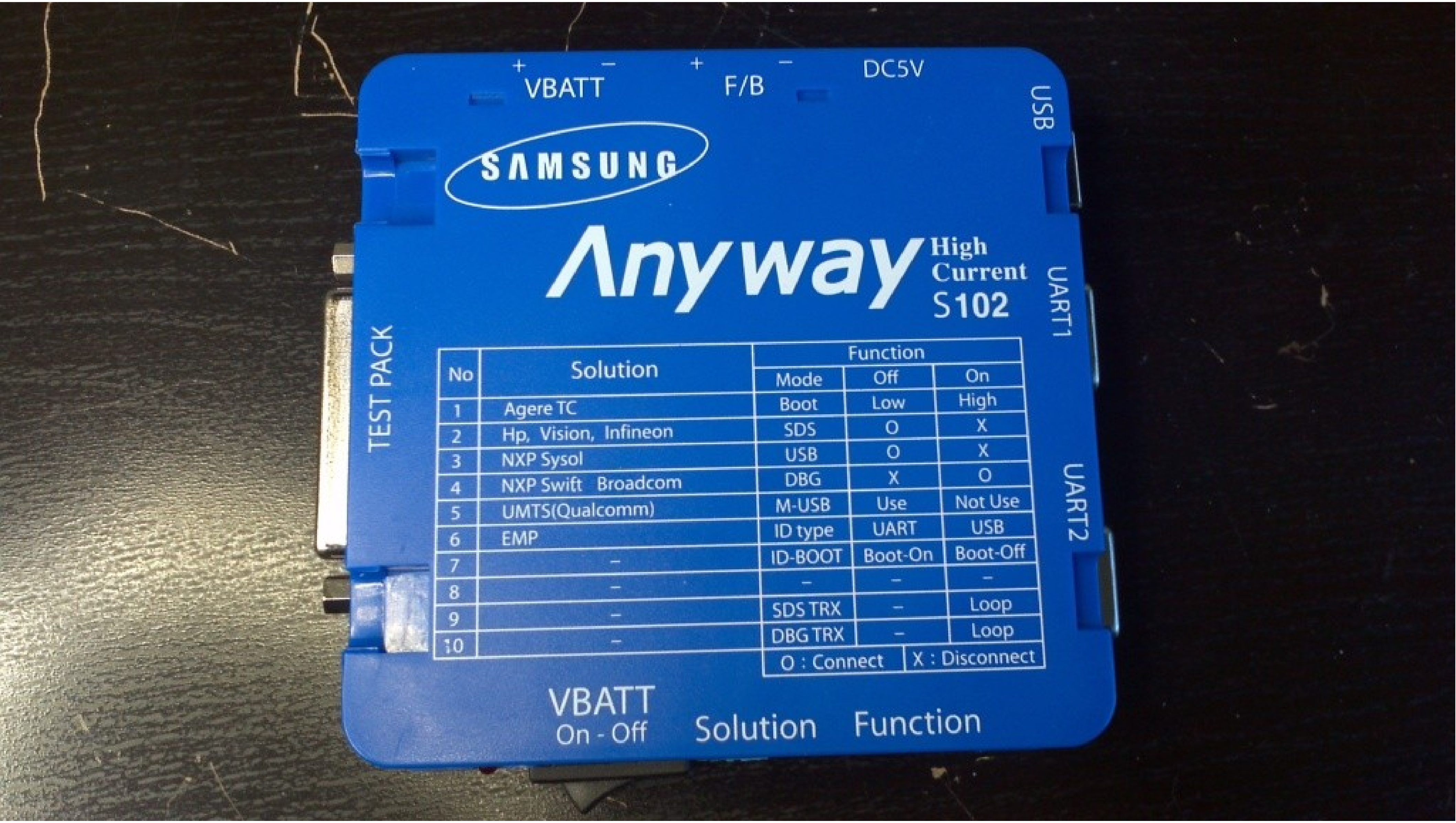
Debug interfaces are meant to be used by someone...

Samsung Anyway S102

supports many phones and tablets

Various cables available

predecessors: S100, S101



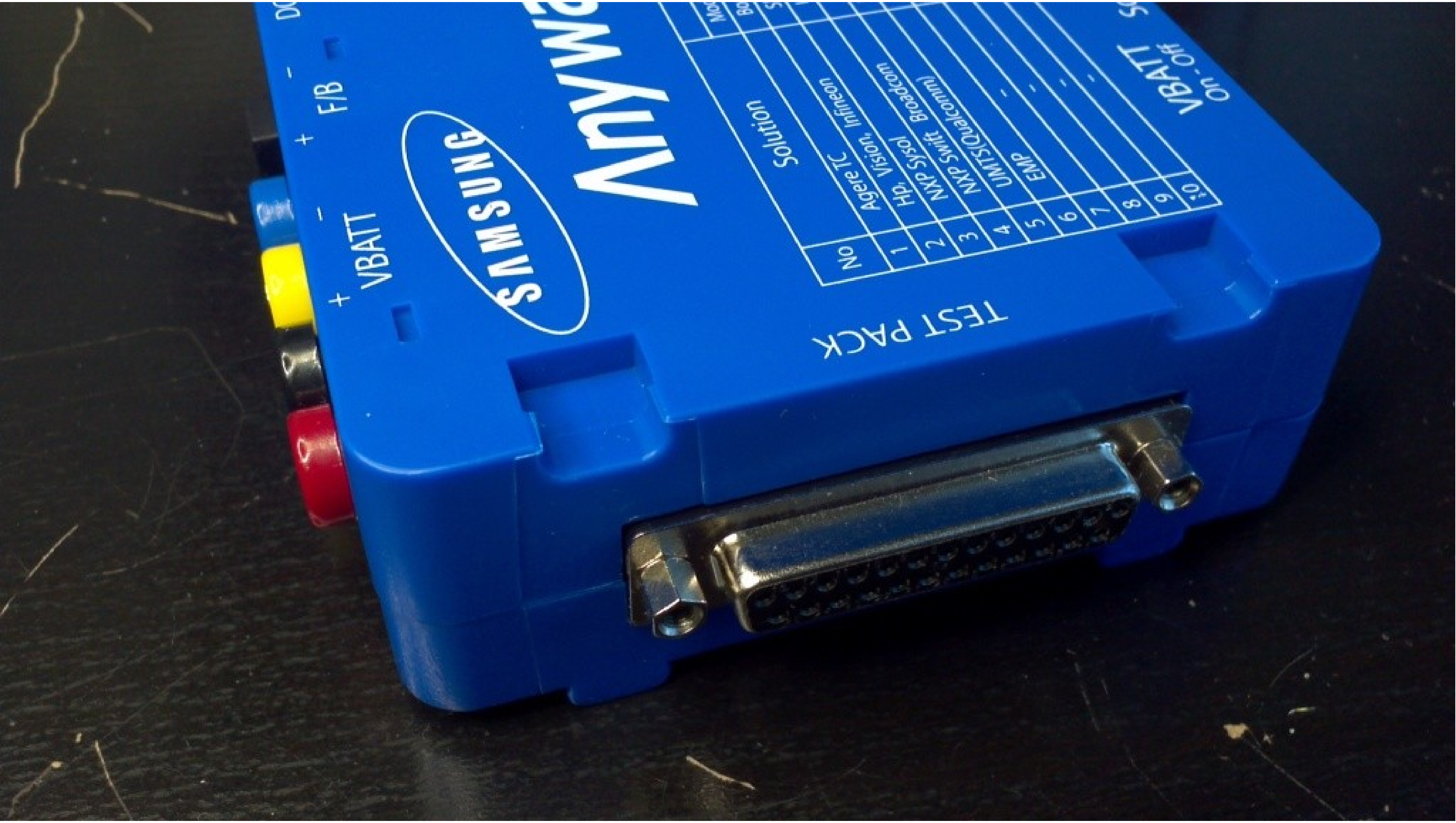
No	Solution	Function		
		Mode	Off	On
1	Agere TC	Boot	Low	High
2	Hp, Vision, Infineon	SDS	O	X
3	NXP Sysol	USB	O	X
4	NXP Swift Broadcom	DBG	X	O
5	UMTS(Qualcomm)	M-USB	Use	Not Use
6	EMP	ID type	UART	USB
7	–	ID-BOOT	Boot-On	Boot-Off
8	–	–	–	–
9	–	SDS TRX	–	Loop
10	–	DBG TRX	–	Loop

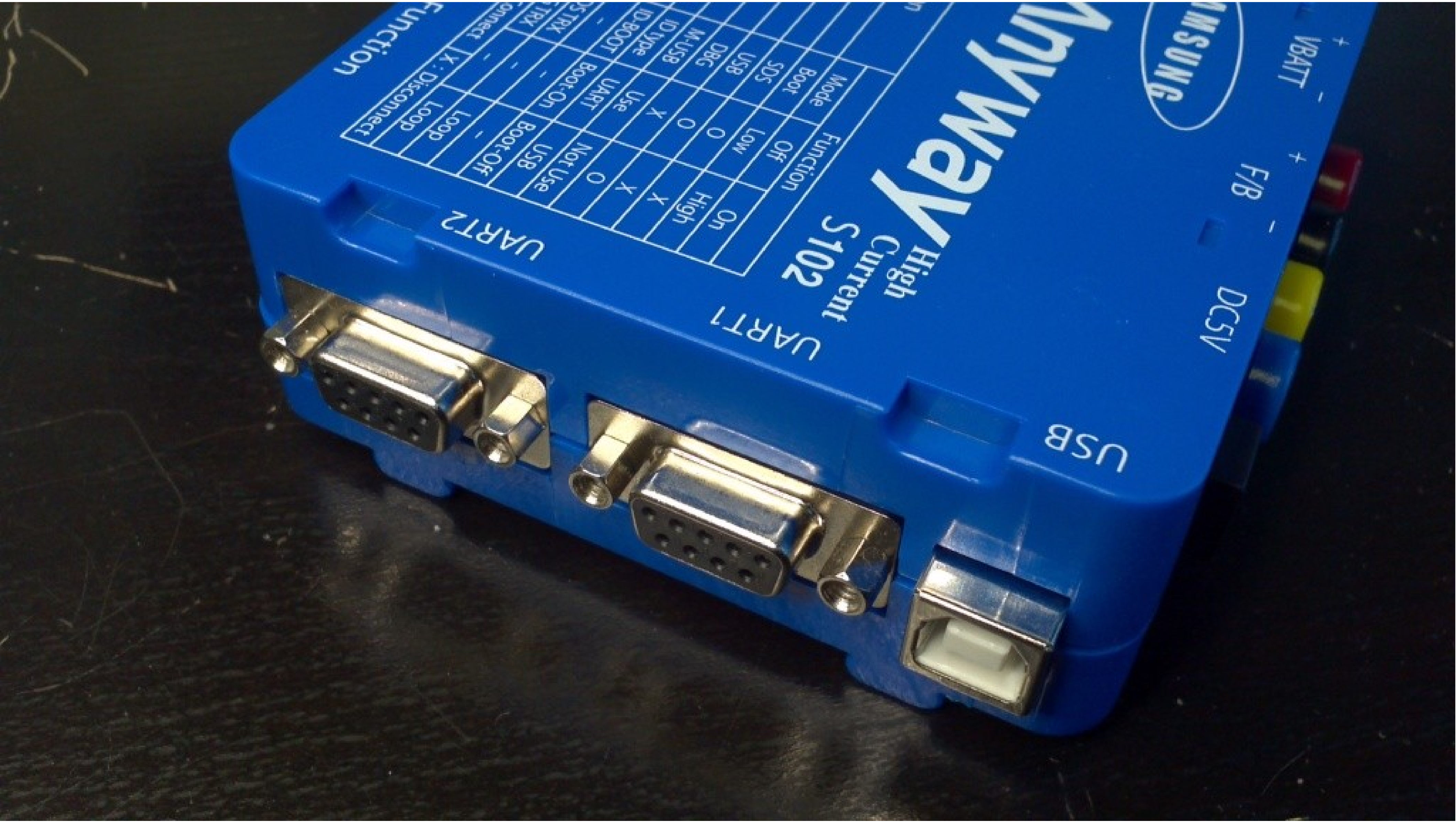
O : Connect X : Disconnect

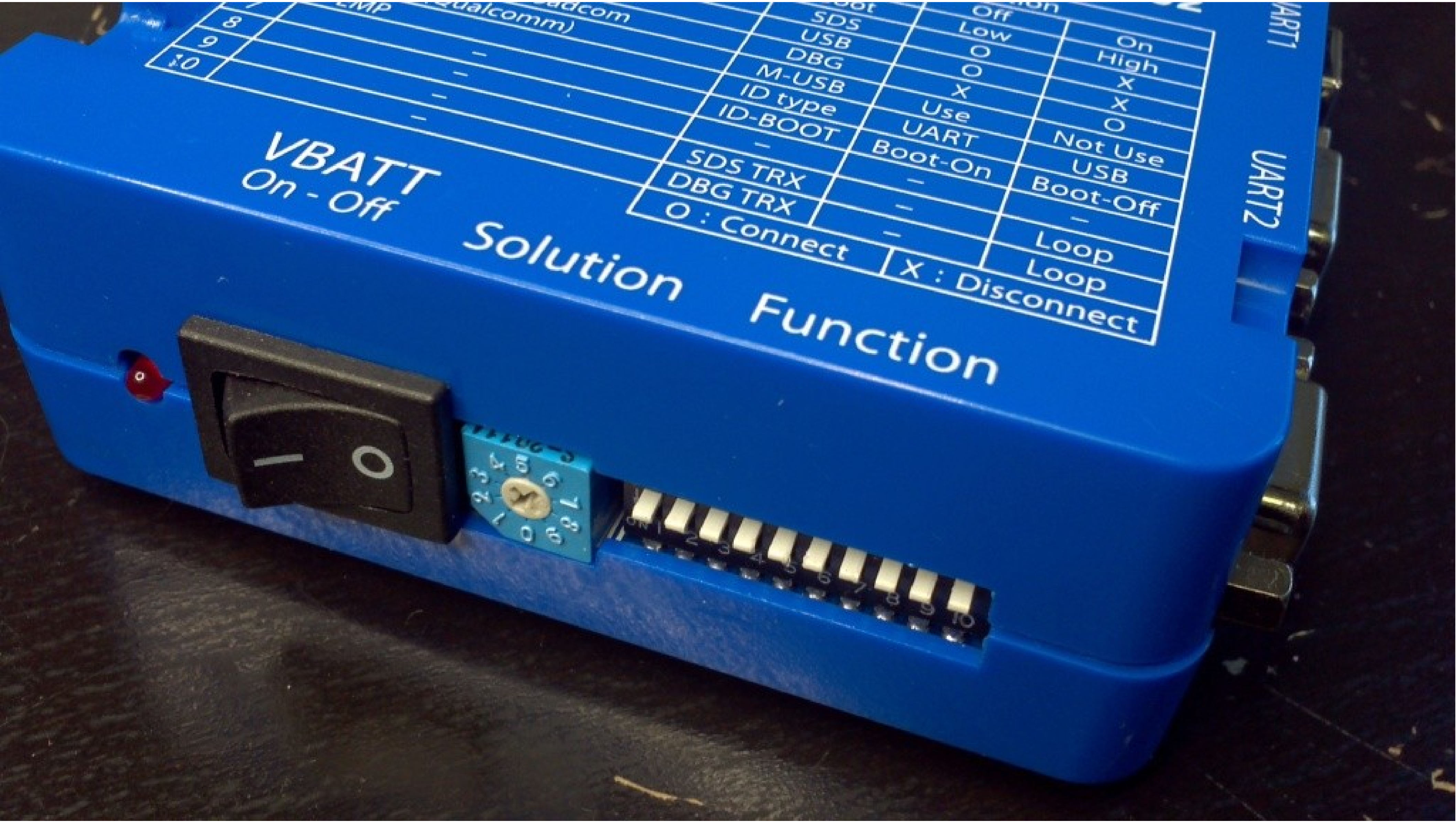
Let's buy it!

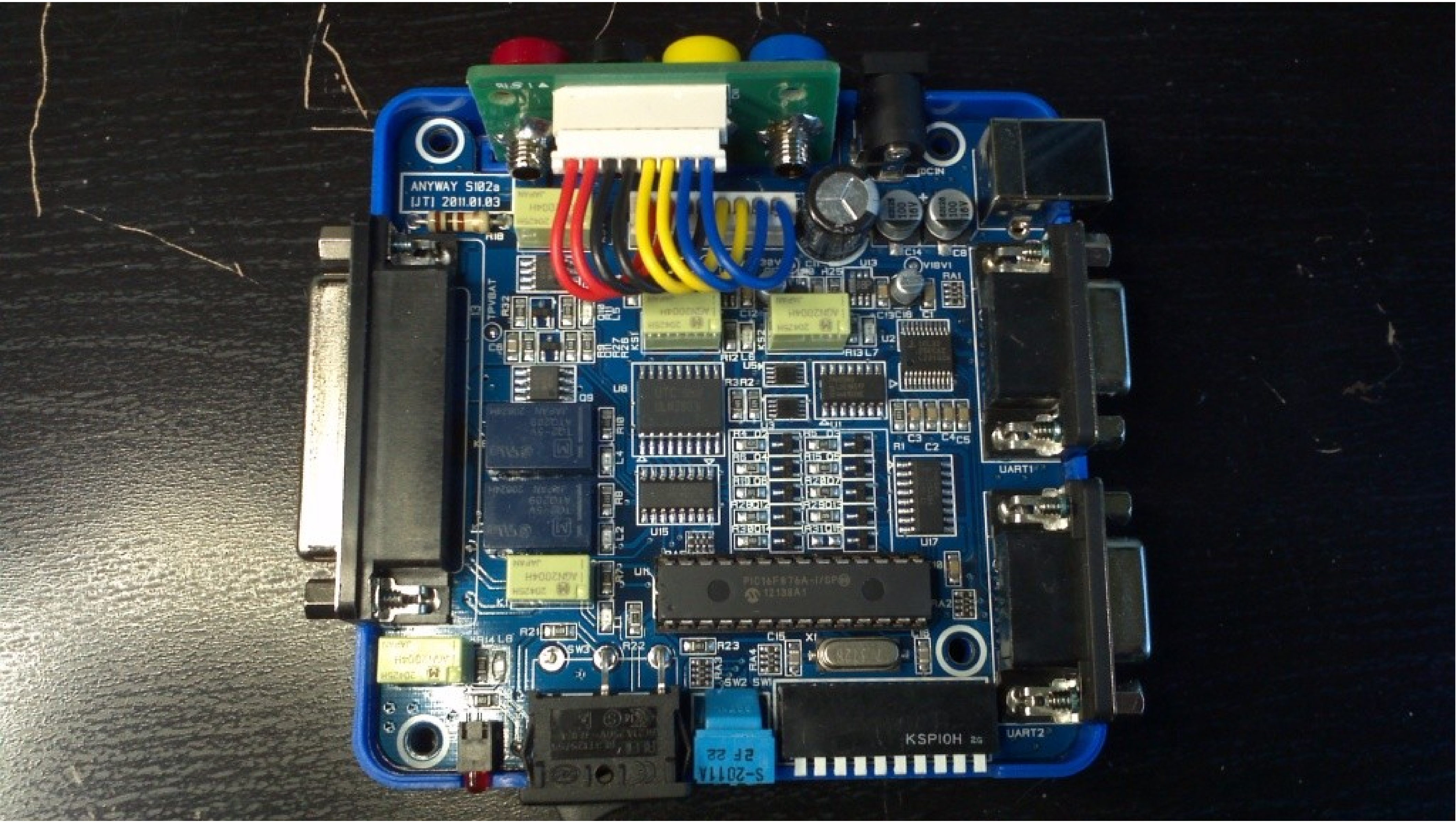
GH99-36900B	$122.50
GH39-01339A (USB)	$37.15
5 V power	$5.95

total under $200

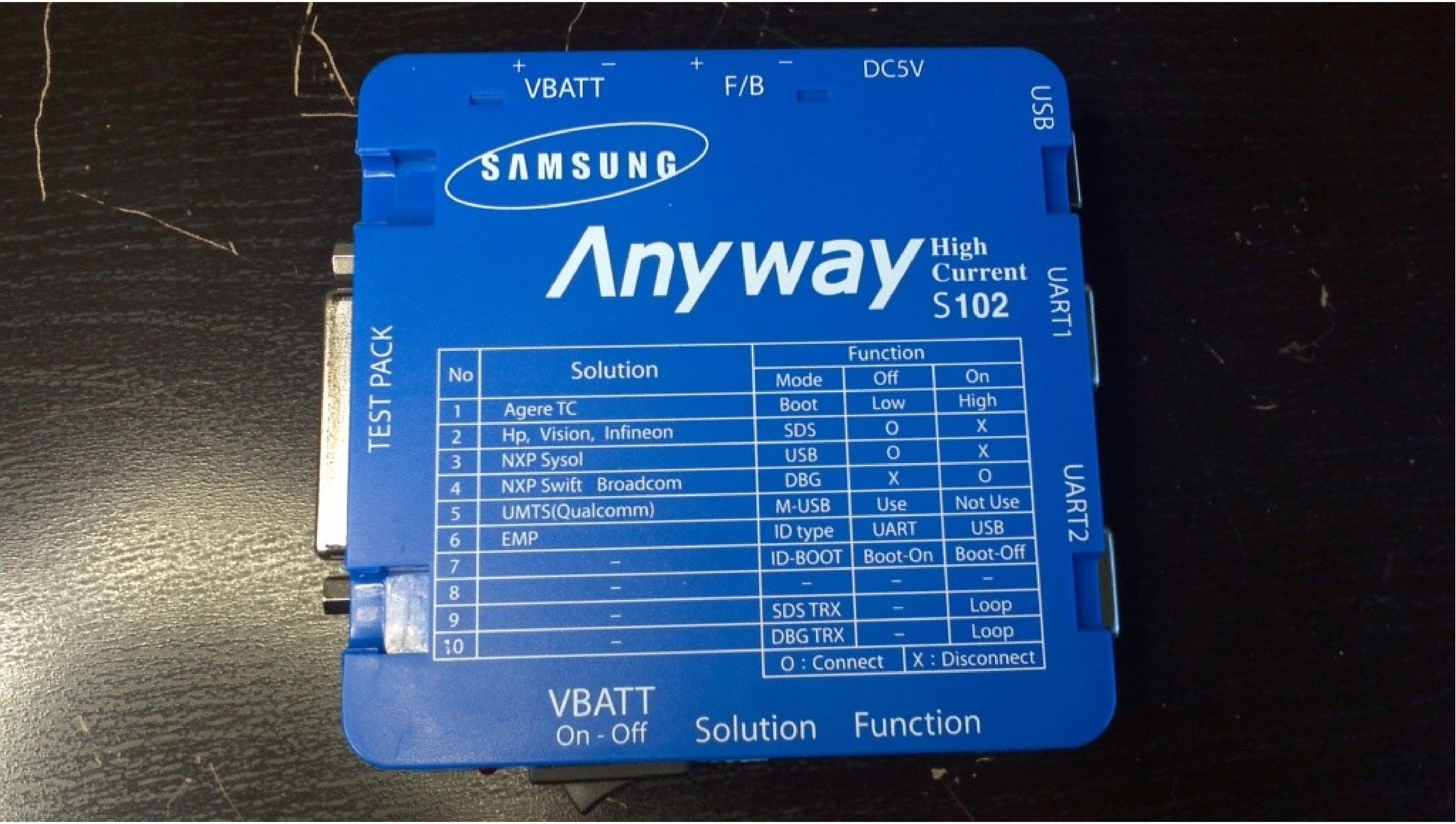

DC
F/B
+
-
VBATT
SAMSUNG
Anywa
No
Solution
1
Agere TC, Vision, Infineon
2
Hp, Sysol, Broadcom
3
NXP Swift, Broadcom
4
NXP Swift(Qualcomm)
5
UMTS
6
EMP
7
8
9
10
VBATT
On-Off
TEST PACK


SAMSUNG
AnyWay
High Current
S102
VBATT
F/B
DC5V
USB
UART1
UART2
Mode
Function
Boot
SDS
USB
DBG
M-USB
ID-type
ID-BOOT
Function
X : Disconnect


8
9
10
(Qualcomm)
SDS
USB
DBG
M-USB
ID type
ID-BOOT
SDS TRX
DBG TRX
O : Connect
X : Disconnect
Off
Low
O
O
X
Use
UART
Boot-On
On
High
X
X
O
Not Use
USB
Boot-Off
Loop
Loop
UART1
UART2
VBATT
On - Off
Solution
Function
ON
1
2
3
4
5
6
7
8
9
10


ANYWAY SI02a
[JT] 2011.01.03
DCIN
UART1
UART2
PIC16F876A-I/SP
KSPIOH
S-2011A

Anyway S102 Functions



No	Solution	Function		
		Mode	Off	On
1	Agere TC	Boot	Low	High
2	Hp, Vision, Infineon	SDS	O	X
3	NXP Sysol	USB	O	X
4	NXP Swift Broadcom	DBG	X	O
5	UMTS(Qualcomm)	M-USB	Use	Not Use
6	EMP	ID type	UART	USB
7	–	ID-BOOT	Boot-On	Boot-Off
8	–	–	–	–
9	–	SDS TRX	–	Loop
10	–	DBG TRX	–	Loop
		O : Connect		X : Disconnect

64.9kΩ	68.15kΩ	Reserved Accessory #5
80.7kΩ	84.1kΩ	DO NOT USE
102kΩ	107.1kΩ	DO NOT USE
121kΩ	127kΩ	TTY Converter
150kΩ	157kΩ	UART Cable
200kΩ	210kΩ	*See Table 4*
255kΩ	268kΩ	Factory Mode Boot OFF-USB[7]
301kΩ	316kΩ	Factory Mode Boot ON-USB[7]
365kΩ	383kΩ	DO NOT USE
442kΩ	464kΩ	*See Table 4*
523kΩ	549kΩ	Factory Mode Boot OFF-UART[7]
619kΩ	650kΩ	Factory Mode Boot ON-UART[7]
1000kΩ	1050kΩ	Audio Type 1 with Remote[8]
1000kΩ	1050kΩ	Audio Type 1 / Only Send End[8]

console

/dev/tty[FIQ]

"shell" user

same user as adb
but without the
same groups

elevate privilege?

```
ser.write("echo '"+tmpread.read()+"' >
 /data/local/tmp/"+filename+'it\n\x03')
```

install APK with pm?

binary exploits
(mempodipper, etc.)?

Ever tried delivering a payload over a slow, unreliable serial console that can only handle 31 input bytes at a time?

smaller payload?

Tiniest_antiguard.apk

4.6 kB

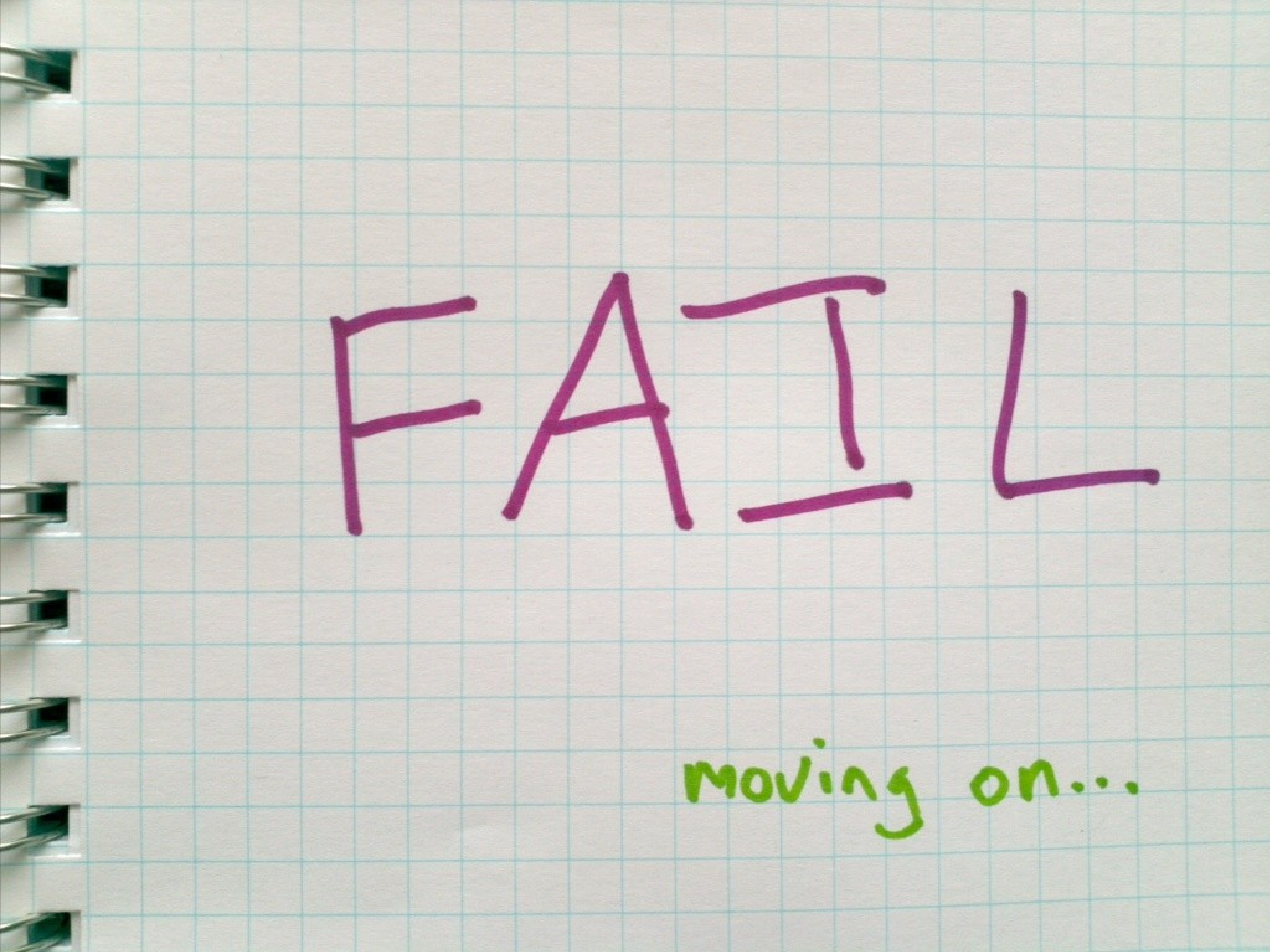
built from previous app
called AntiGuard

17 kB → stripped functions

→ compiled → decompiled to smali

→ stripped more → re compiled

→ signed → 4.6 kB



FAIL

moving on...

no wget

no netcat

DNS TXT?

SSIDs???

/system/bin/adb ?

- adb client on newer phones
- allows remote adb instance
- network adb pull?

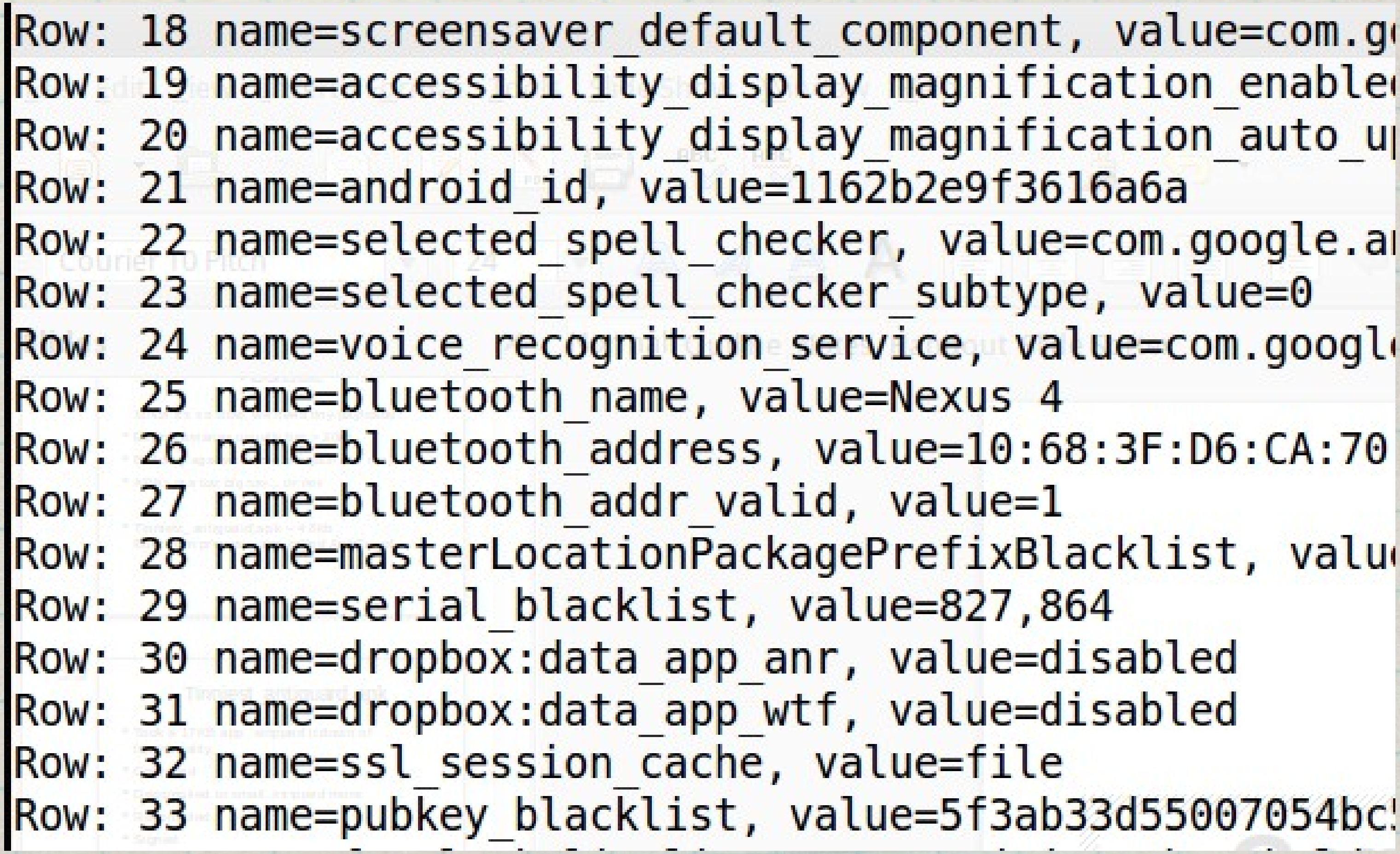
other options

```
# Select "name" and "value" columns from secure
settings where "name" is equal to "new_setting" and
sort the result by name in ascending order.

adb shell content query --uri
content://settings/secure --projection name:value
--where "name='new_setting'" --sort "name ASC"
```

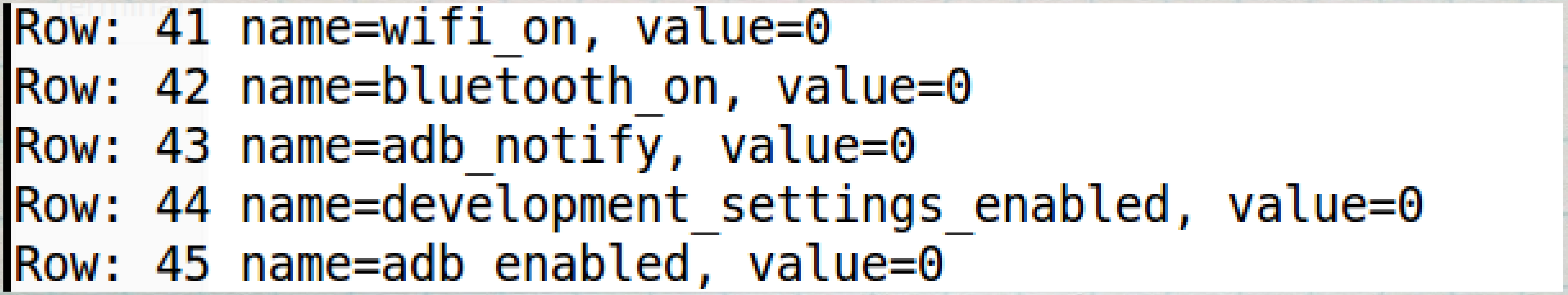
```
data/data/com.android.provers.settings/
databases/settings.db (sqlite)
```

content

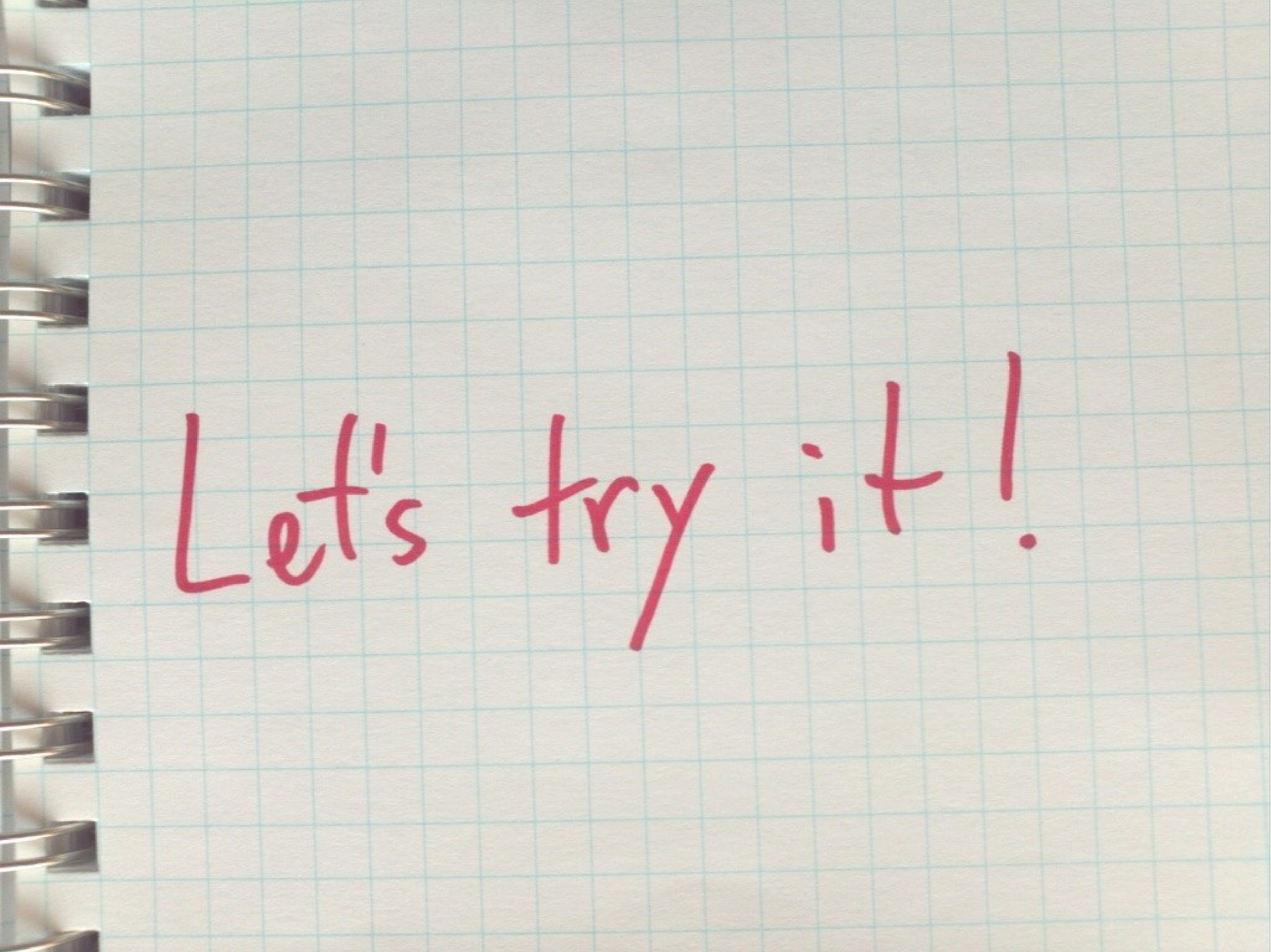


```
Row: 18 name=screensaver_default_component, value=com.g
Row: 19 name=accessibility_display_magnification_enable
Row: 20 name=accessibility_display_magnification_auto_u
Row: 21 name=android_id, value=1162b2e9f3616a6a
Row: 22 name=selected_spell_checker, value=com.google.a
Row: 23 name=selected_spell_checker_subtype, value=0
Row: 24 name=voice_recognition_service, value=com.googl
Row: 25 name=bluetooth_name, value=Nexus 4
Row: 26 name=bluetooth_address, value=10:68:3F:D6:CA:70
Row: 27 name=bluetooth_addr_valid, value=1
Row: 28 name=masterLocationPackagePrefixBlacklist, valu
Row: 29 name=serial_blacklist, value=827,864
Row: 30 name=dropbox:data_app_anr, value=disabled
Row: 31 name=dropbox:data_app_wtf, value=disabled
Row: 32 name=ssl_session_cache, value=file
Row: 33 name=pubkey_blacklist, value=5f3ab33d55007054bc
```

context



```
Row: 41 name=wifi_on, value=0
Row: 42 name=bluetooth_on, value=0
Row: 43 name=adb_notify, value=0
Row: 44 name=development_settings_enabled, value=0
Row: 45 name=adb enabled, value=0
```



Let's try it!

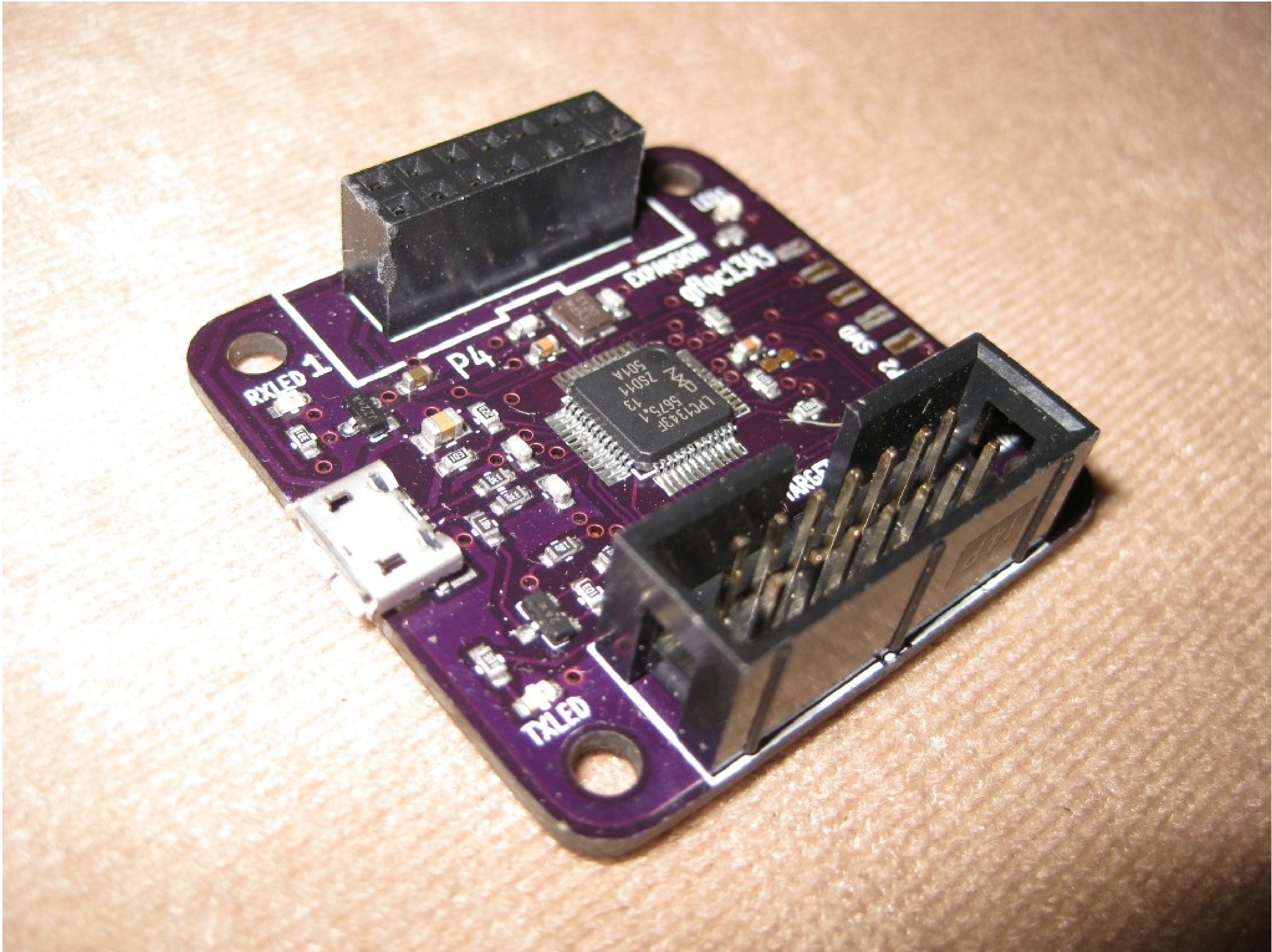
Automated Probing

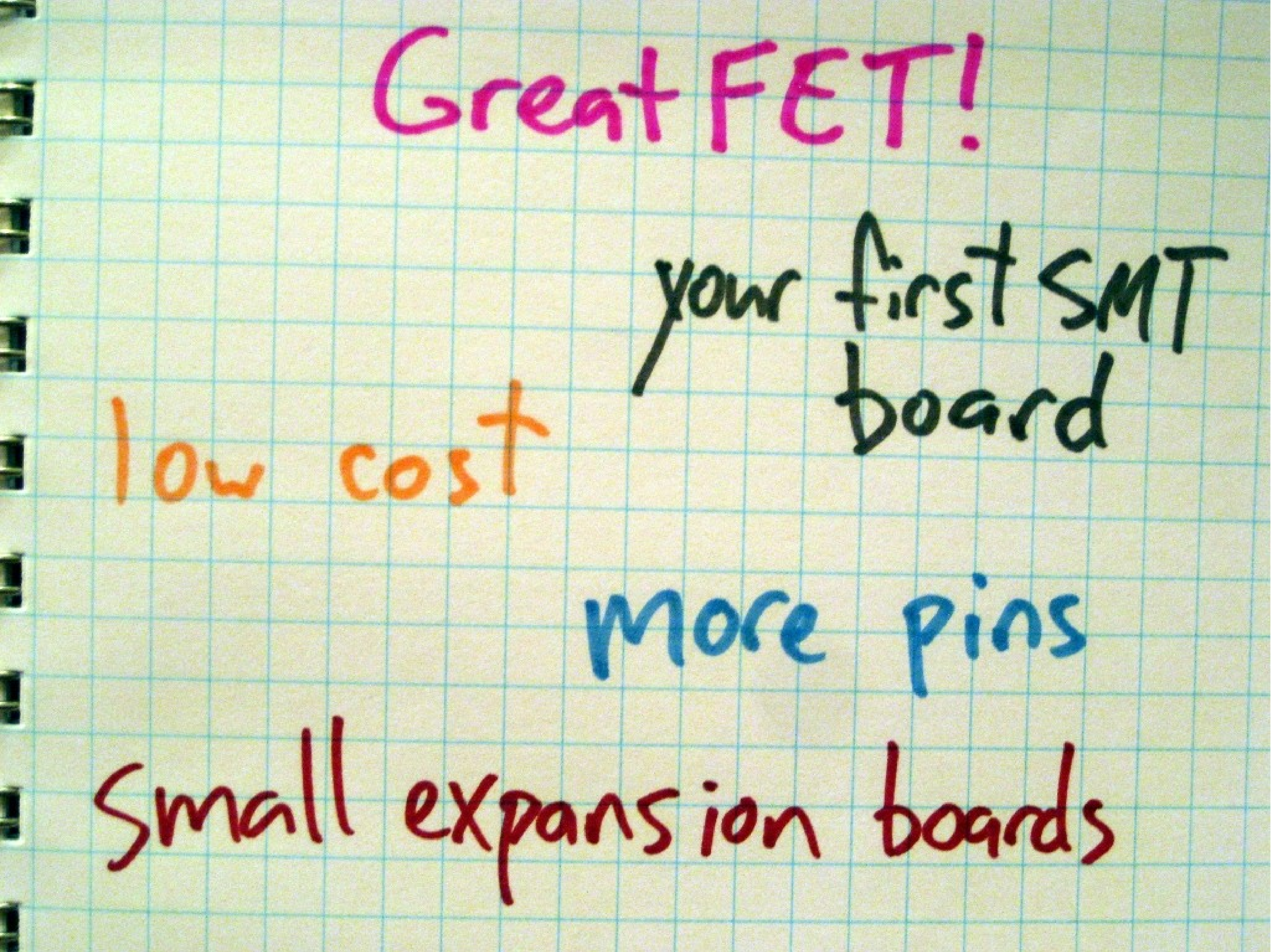
Bus Pirate?

GoodFET?

Datenkrake?

JTAGulator?


RXLED 1
P4
EXPANSION
LPC1343F
TXLED



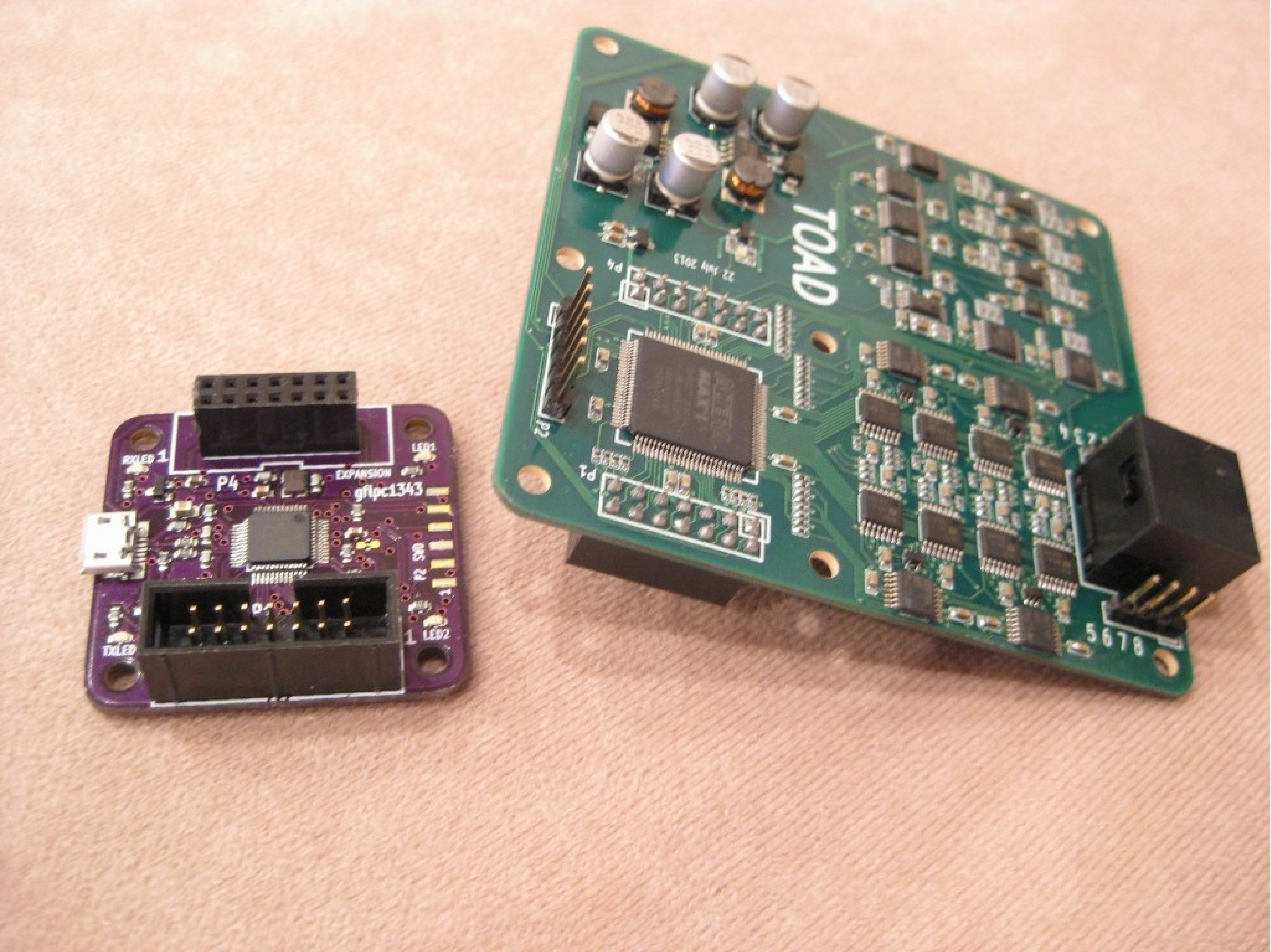
Great FET!

your first SMT board

low cost

more pins

small expansion boards

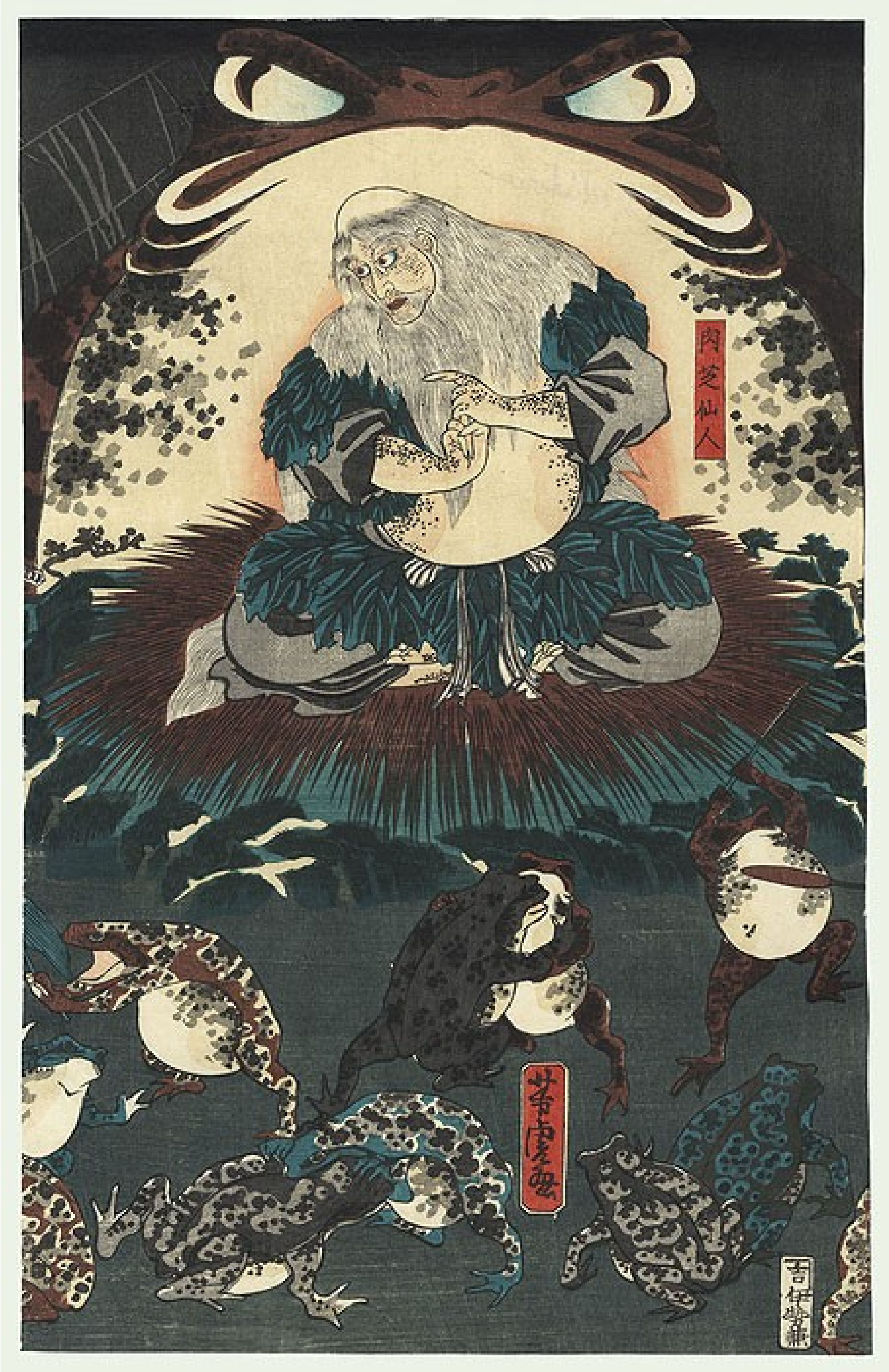

TOAD
22 July 2013
P4
P2
P1
5678
RXLED 1
LED1
P4
EXPANSION
gflpc1343
SWD
P2
1
LED2
TXLED

TOAD

Totally Overengineered Adapter/Detector

NINJA TOAD!!!

http://fc03.deviantart.net/fs71/f/2010/221/e/8/NINJA_TOAD_by_TartarusWolf.jpg



http://www.fujiarts.com/japanese-prints/k147/277k147f.jpg

UART

arbitrary voltage
0-5V

non-UART stuff

configurable resistance between pins

ADC

arbitrary pin-out

negative voltages

RS-232 levels (up to ± 15V)

Questions?

http://grantscottgadgets.com/infiltrate2013