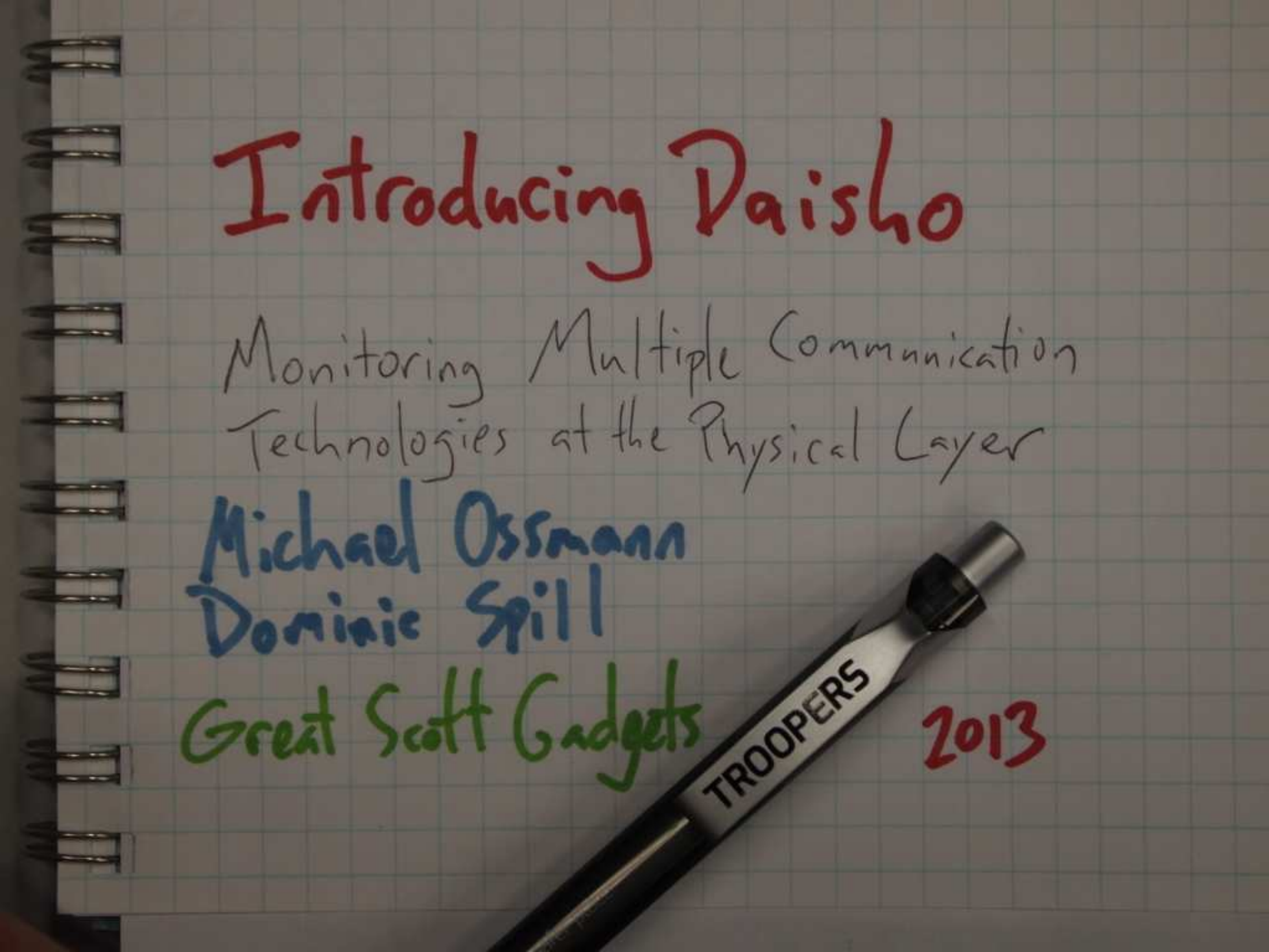
Introducing Daisho

Monitoring Multiple Communication Technologies at the Physical Layer

Michael Ossmann
Dominic Spill

Great Scott Gadgets

2013



The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

The Team

Jared Boone

Marshall Hecht

Mike Kershaw

Michael Ossmann

Dominic Spill

Benjamin Vernoux

"Security will not get better until tools for practical exploration of the attack surface are made available."

– Joshua Wright

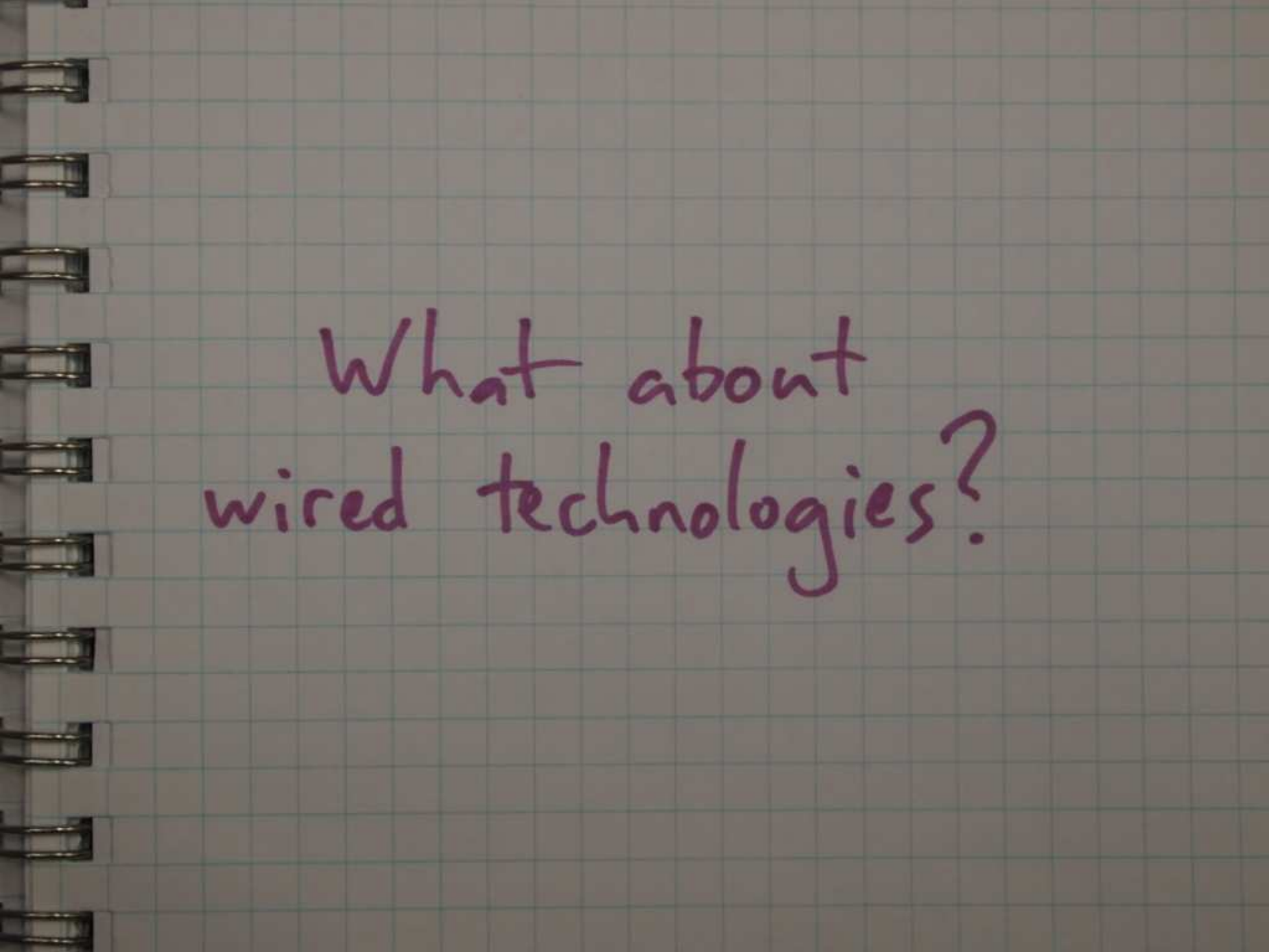
Wi-Fi

~~WEP~~ → WPA

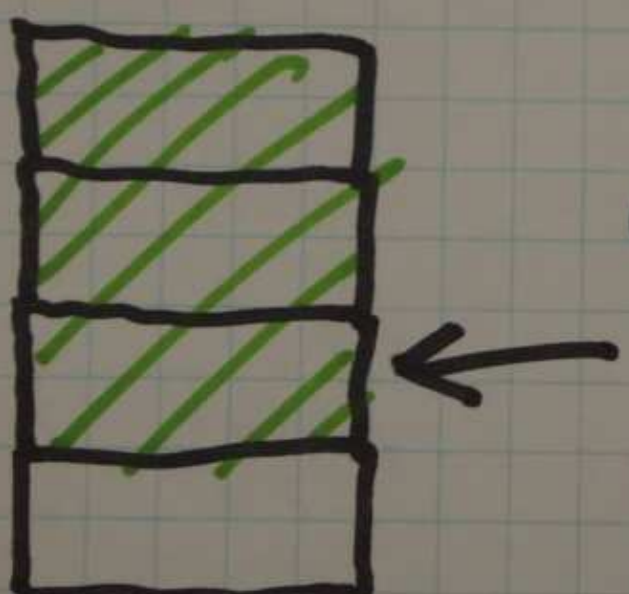
~~WPA~~ → WPA2

Bluetooth

~~PIN~~ → Secure Simple Pairing


What about
wired technologies?

Physical Layer Access



sniffer monitors one layer and every layer above

Target Technologies

1000BASE-T

USB 3.0

HDMI

RS-232

and more!

Existing Monitors: Ethernet

Throwing Star LAN Tap : low speed

mirrored switch port : visible to target

software tap : higher layer

Existing Monitors: USB

Beagle: expensive, closed source

USBEE: low speed

OpenVizsla: vaporware

Existing Monitors: HDMI

NeTV: no monitoring, low speed

Bus Pirate: only control signals

VideoGhost: still images

Drawbacks of Existing Monitors

closed source

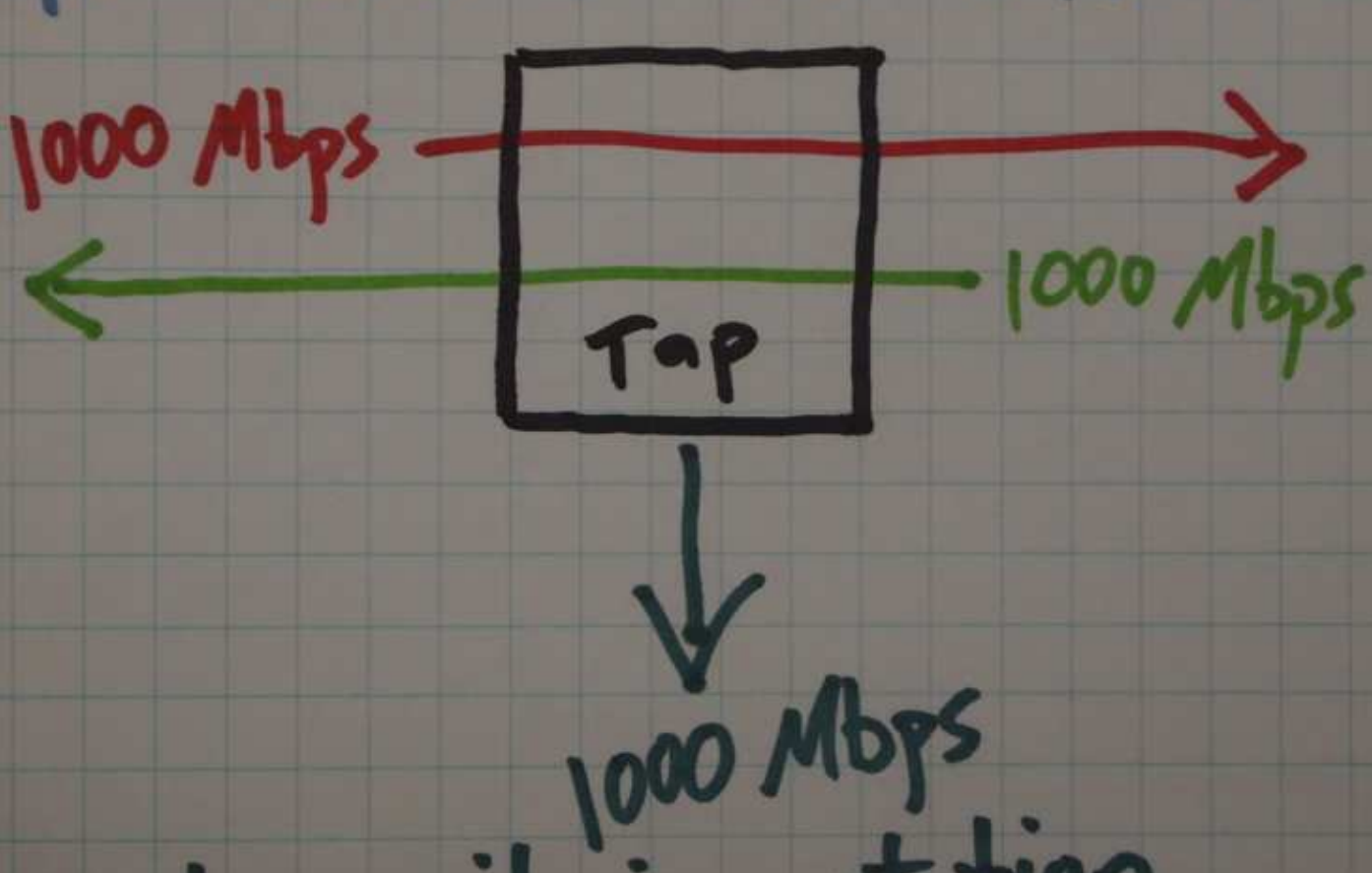
inadequate performance

expensive

not portable

link layer or higher

1000BASE-T Bottleneck



we need

open source

high performance

affordable

portable

physical layer

modular

integration

(wireshark, etc.)

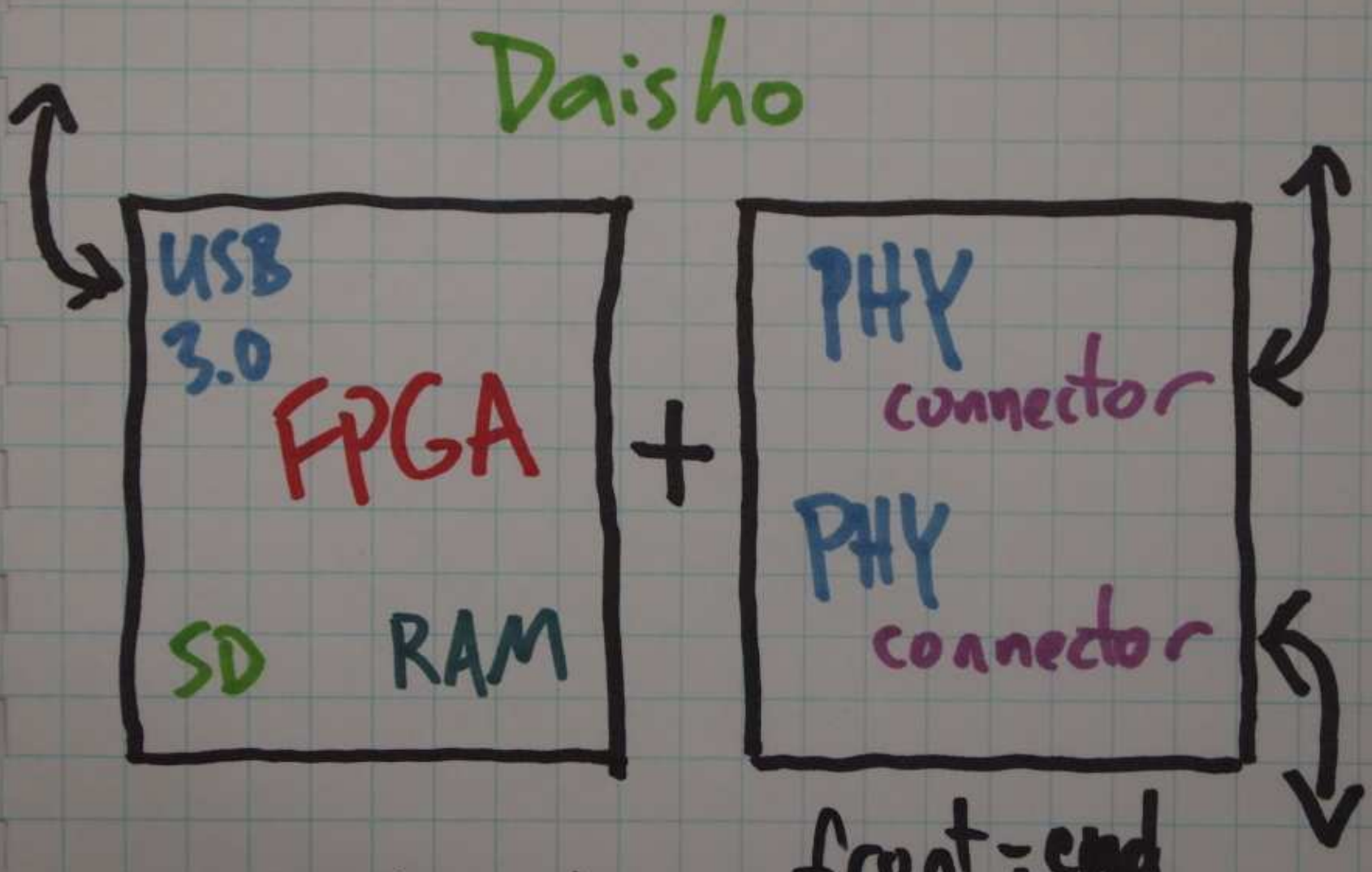
Daisho

off-the-shelf PHY components

SuperSpeed USB 3.0 to host

FPGA

extensible, modular design


Daisho
USB
3.0
FPGA
SD
RAM
+
PHY
connector
PHY
connector
mainboard
front-end
module

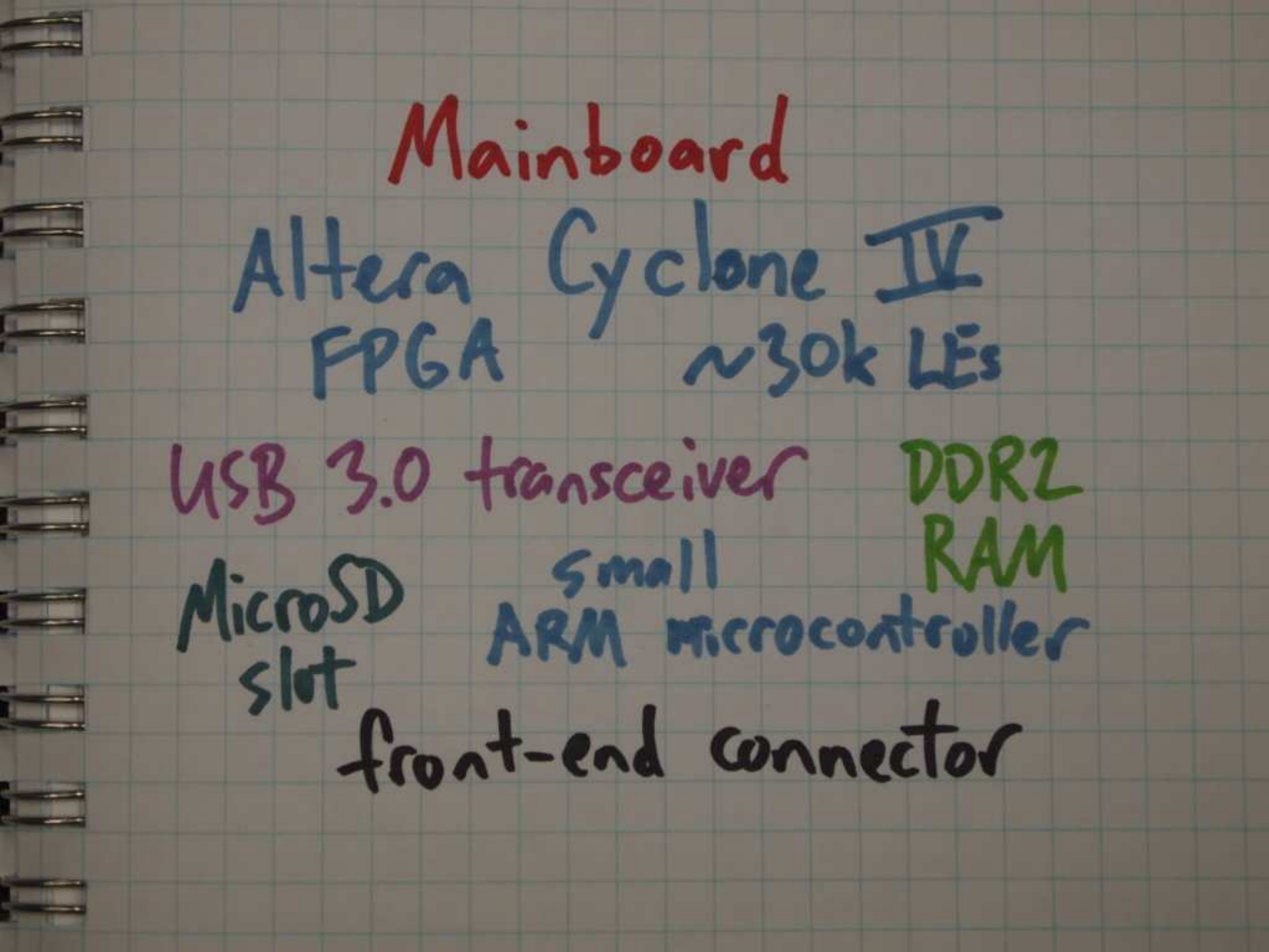
Open Source

software

hardware

FPGA cores

everything is
on GitHub


Mainboard
Altera Cyclone IV
FPGA
~30k LEs
USB 3.0 transceiver
DDR2
RAM
MicroSD
slot
small
ARM microcontroller
front-end connector

USB 3.0 to Host

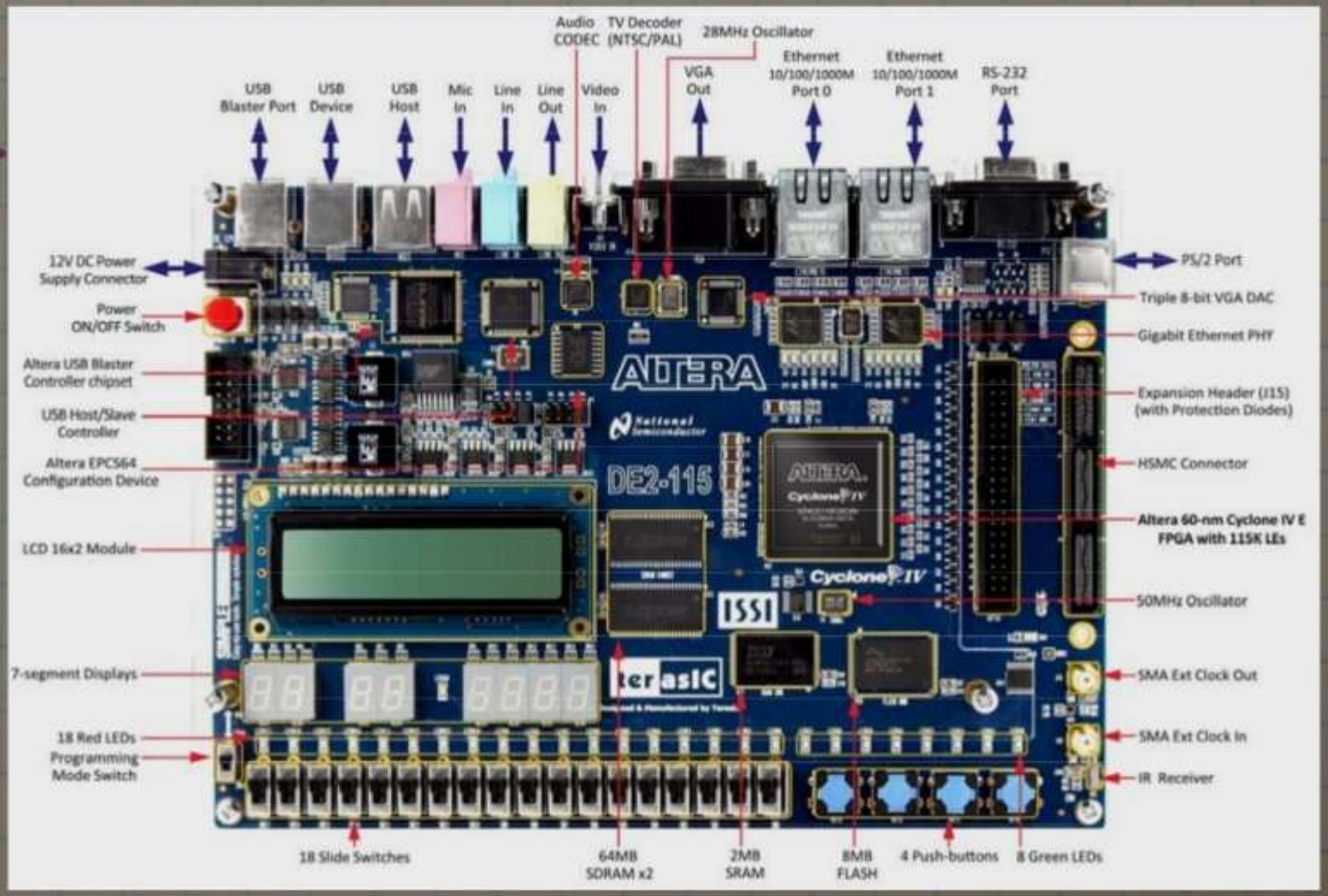
Texas Instruments

TUSB1310A

World's first open source USB 3.0 device core

Development Platform

Terasic DE2-115



RS-232 Module

dual connection

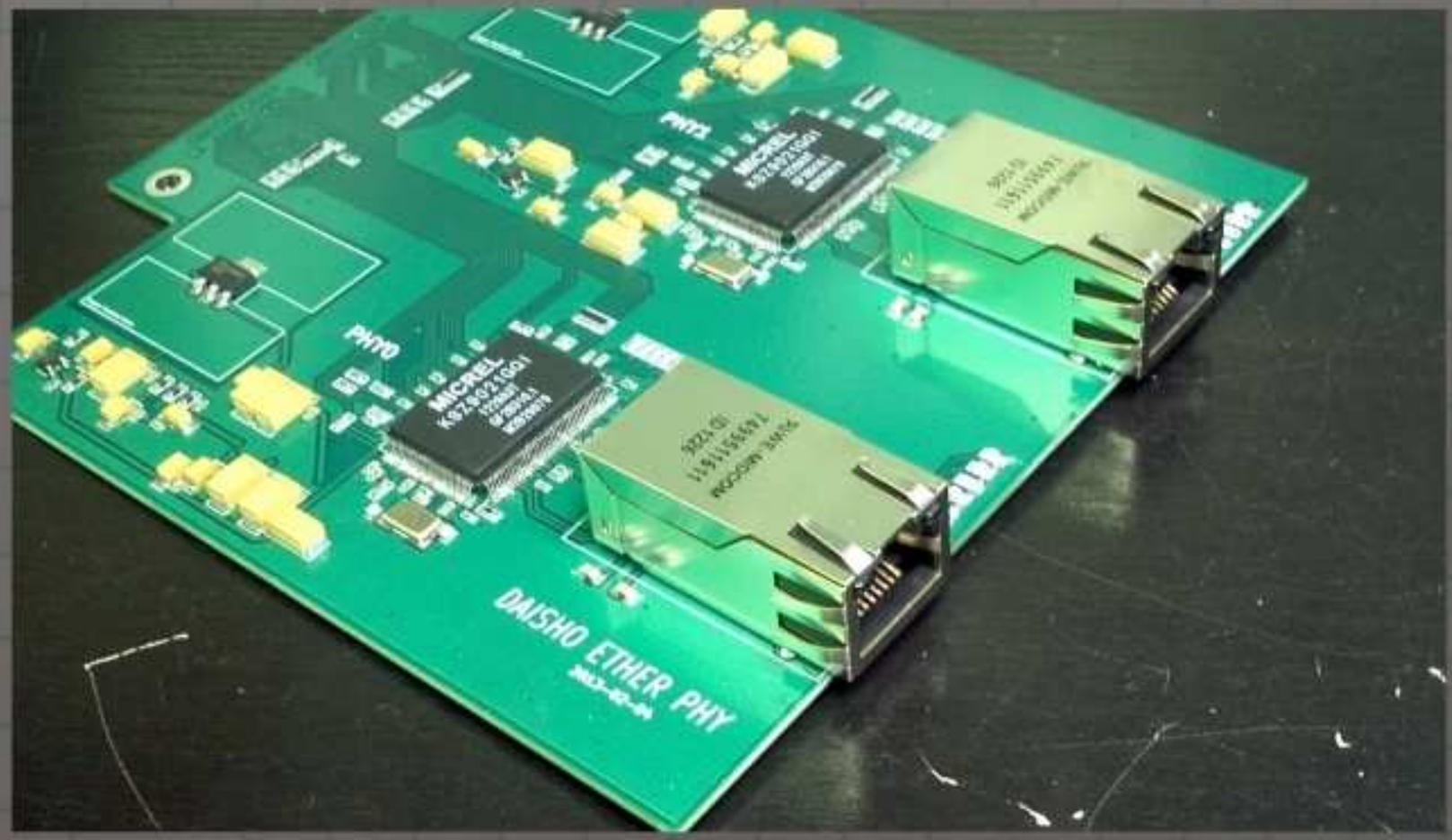
2x DTE
(ADM3307E)

2x DCE
(ADM3310E)

1000BASE-T Module

2x PHY

(KSZ9021GQ)



HDMI Module

Generic high speed SerDes

everything else on FPGA

expect to support pixel clocks up to 340 MHz (HDMI 1.4 maximum)

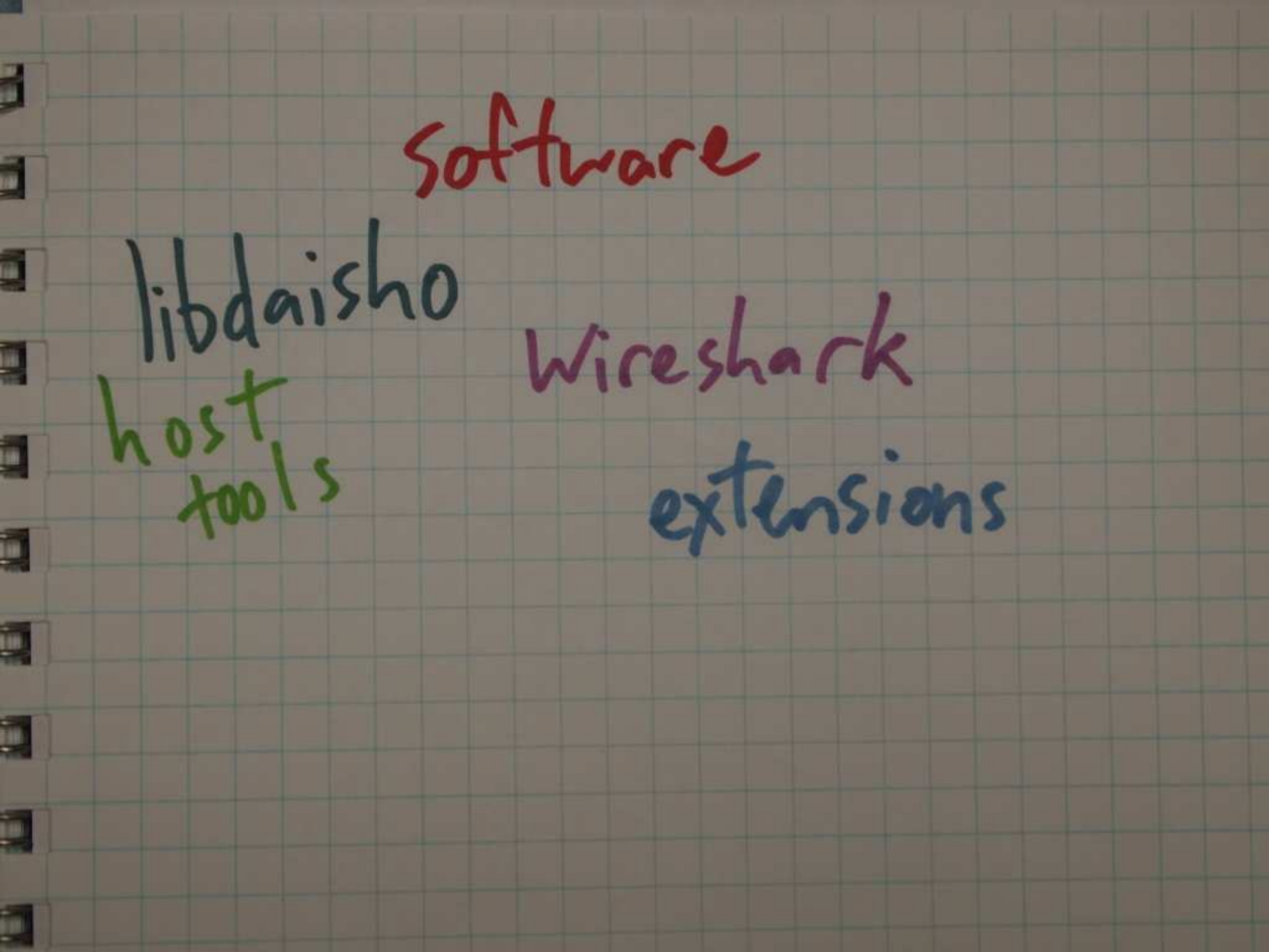
USB 3.0 Module

Greatest challenge!

2x TusB1310A

had to get a bigger front-end connector


Dominstration

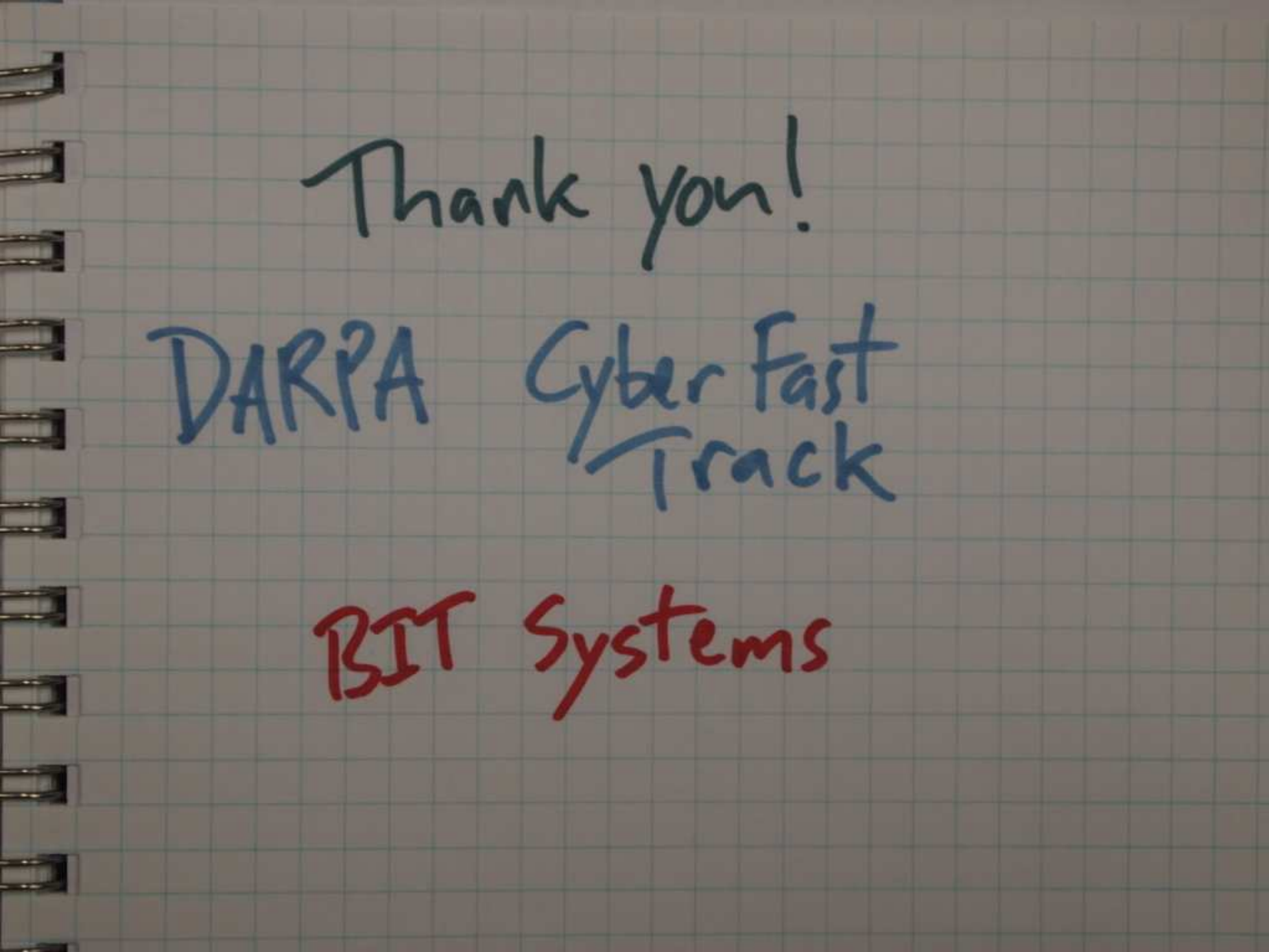

software
libdaisho
Wireshark
host
tools
extensions


Future Targets?
DisplayPort
SATA
DVI
SAS
telephone/DSL
more!

Third Party Modules

What can you do with USB 3.0 and an FPGA?

Wideband SDR?


Thank you!
DARPA Cyber Fast Track
BIT Systems

http://greatscottgadgets.com/

https://github.com/mossmann/daisho

#daisho on freenode.net