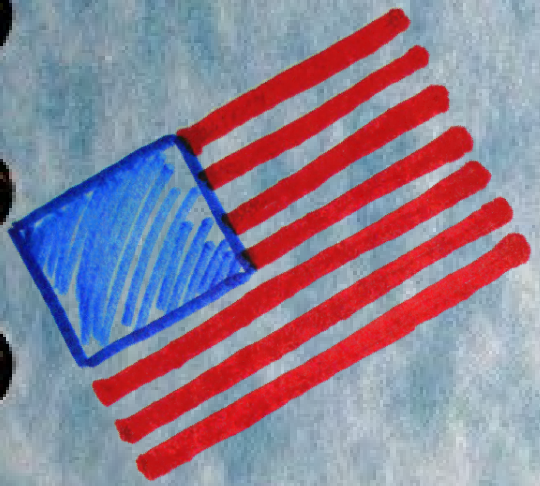
Bluetooth
smells like chicken





Dominic Spill
Michael Ossmann
Mark Steward

I'm Dominic



Imperial College London

dominicgs@gmail.com

I'm Mark



markstewardegmail.com

I'm Mike



Institute for
Telecommunication Sciences

mike@ossmann.com

Certain commercial equipment, materials, and software are identified to specify technical aspects of the reported procedures and results. In no case does such identification imply recommendations or endorsement by the U.S. Government, its departments, or its agencies; nor does it imply that the equipment, materials, and software identified are the best available for this purpose.

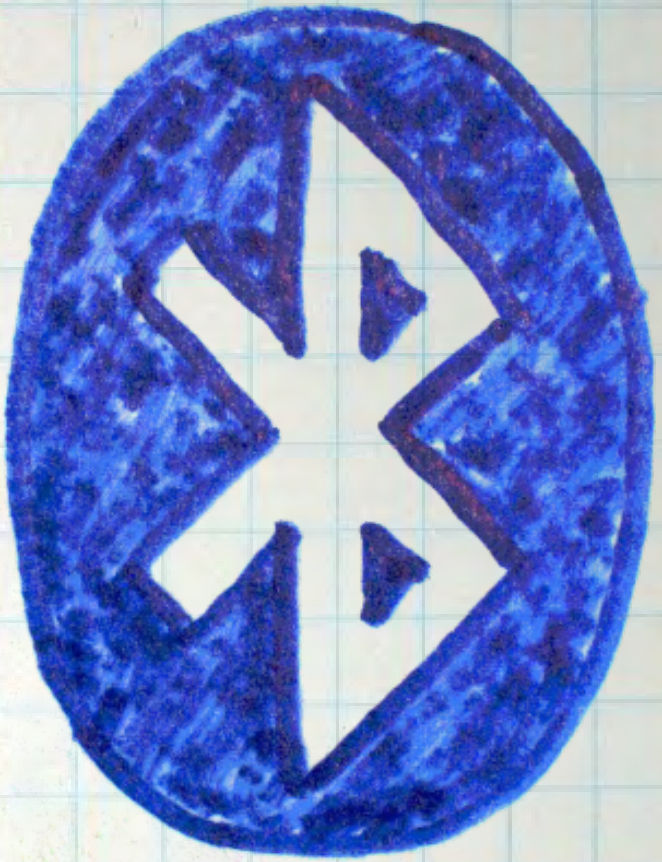

Sniffing
Bluetooth
is
Hard

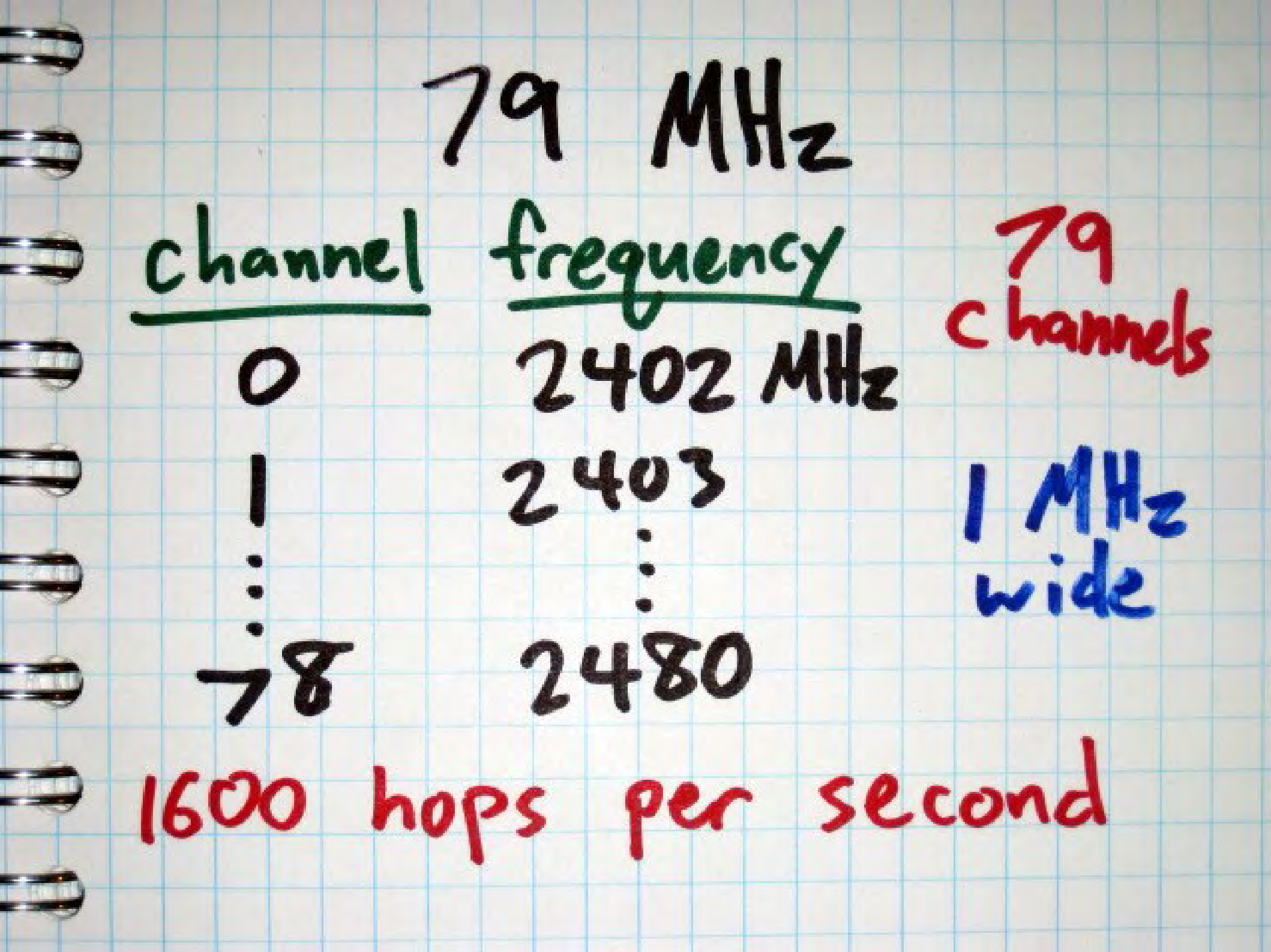
Bluetooth

PAN

2.4 GHz

Frequency Hopping




79 MHz
channel
frequency
0
2402 MHz
1
2403
78
2480
79 channels
1 MHz wide
1600 hops per second

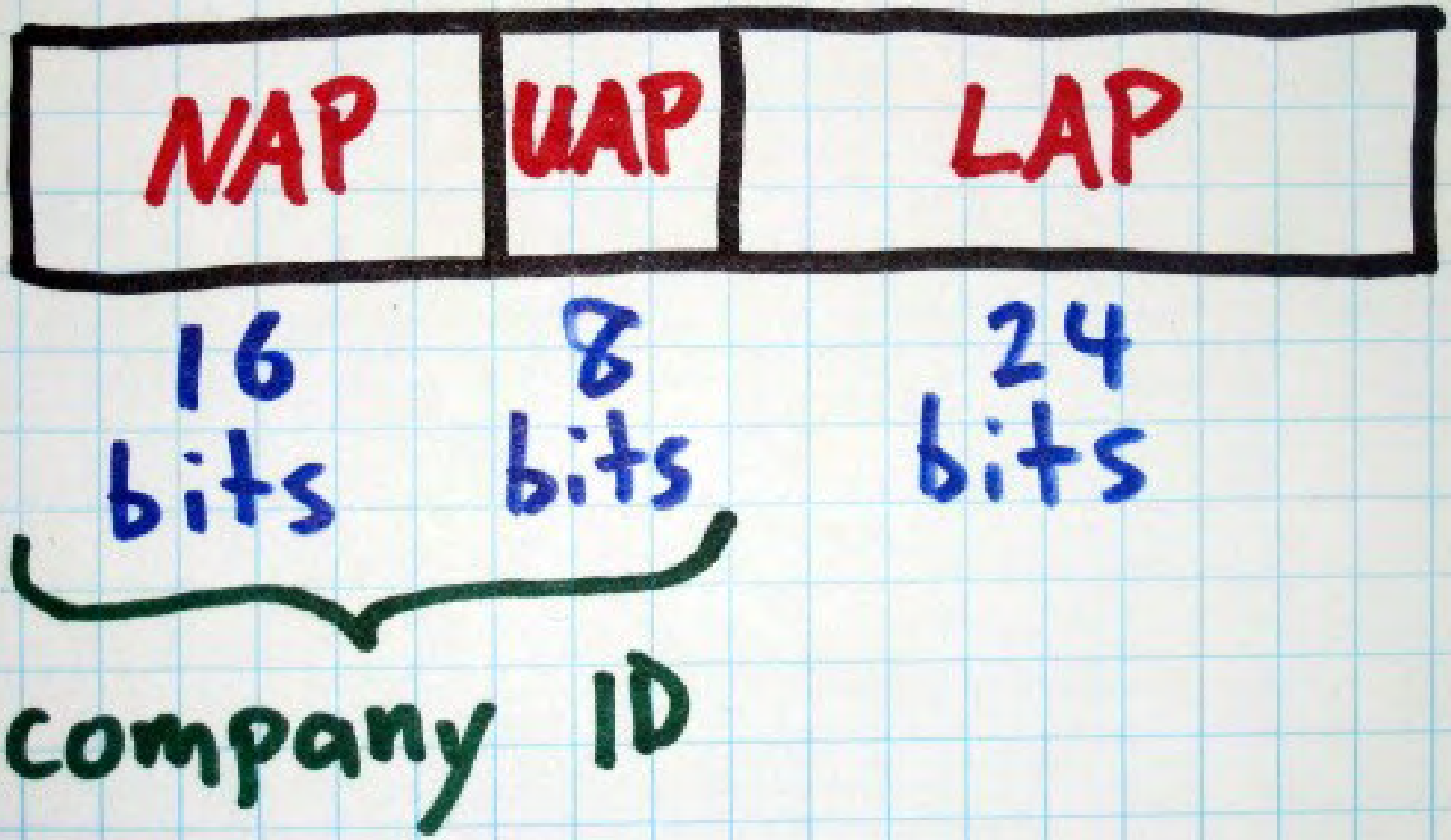
Clocks

increment 3200 times / second

hops every other clock

master device provides clock for piconet

BD_ADDR



sniffing hardware

protocol analyzer
$10,000

Bluetooth OEM
$10

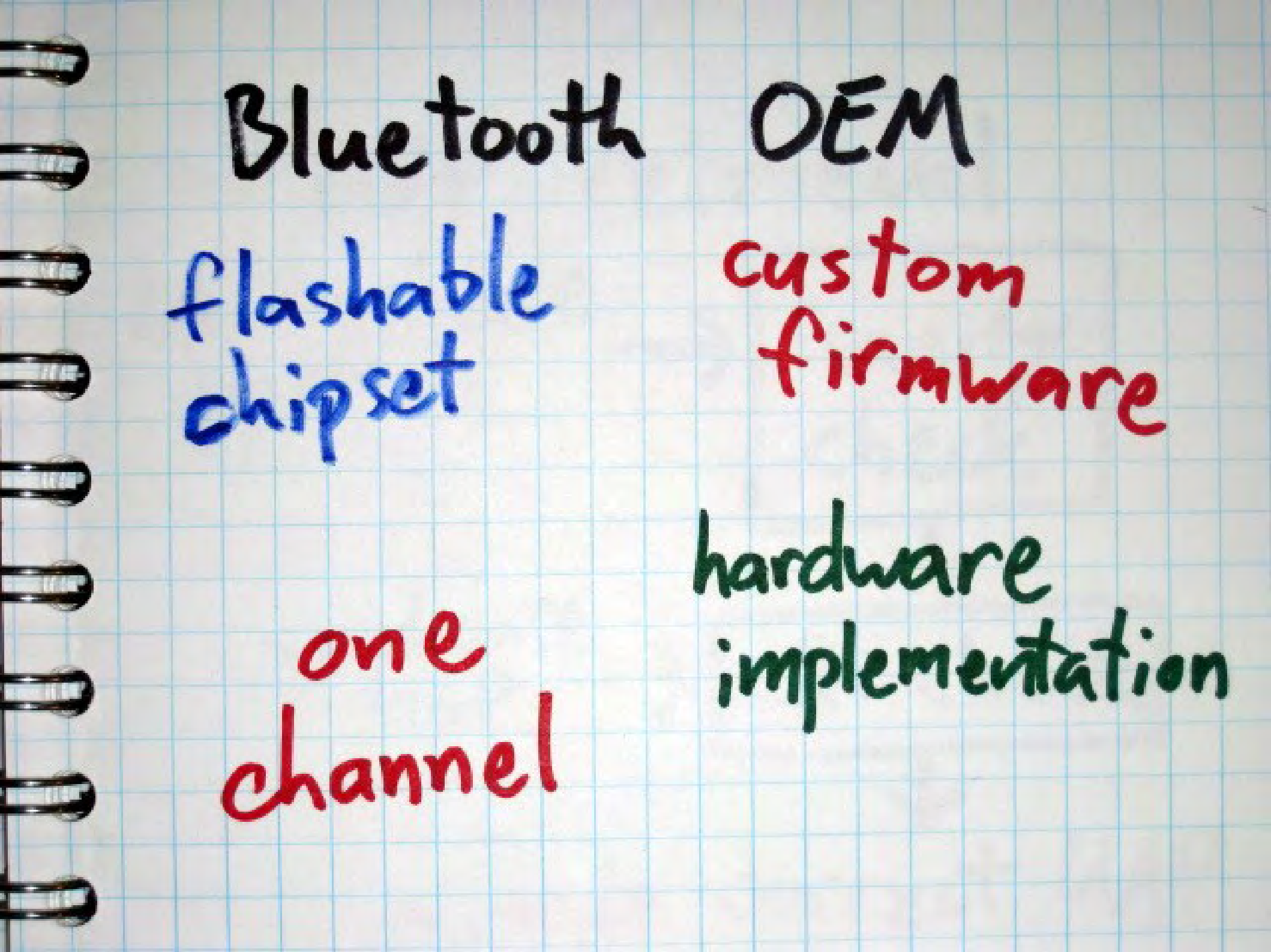
USRP
$1000

Protocol analyzer

test equipment for Bluetooth manufacturers

expensive or illegal

doesn't do what we want


Bluetooth
OEM
flashable chipset
custom firmware
hardware implementation
one channel

software radio

wideband receiver

USRP 8MHz

USRP2 25MHz

GNU Radio

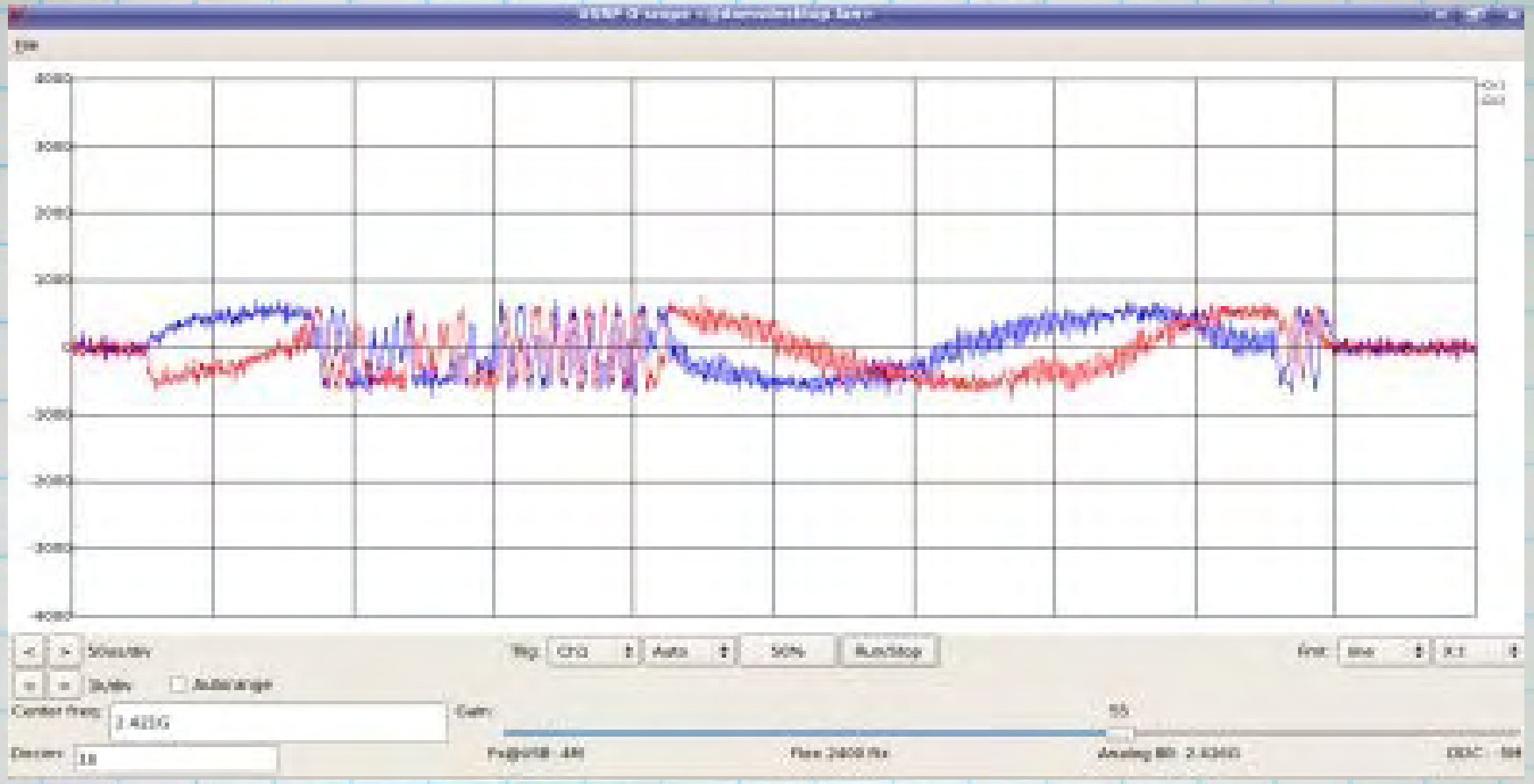
software signal processing

we can do what we want

this has potential...

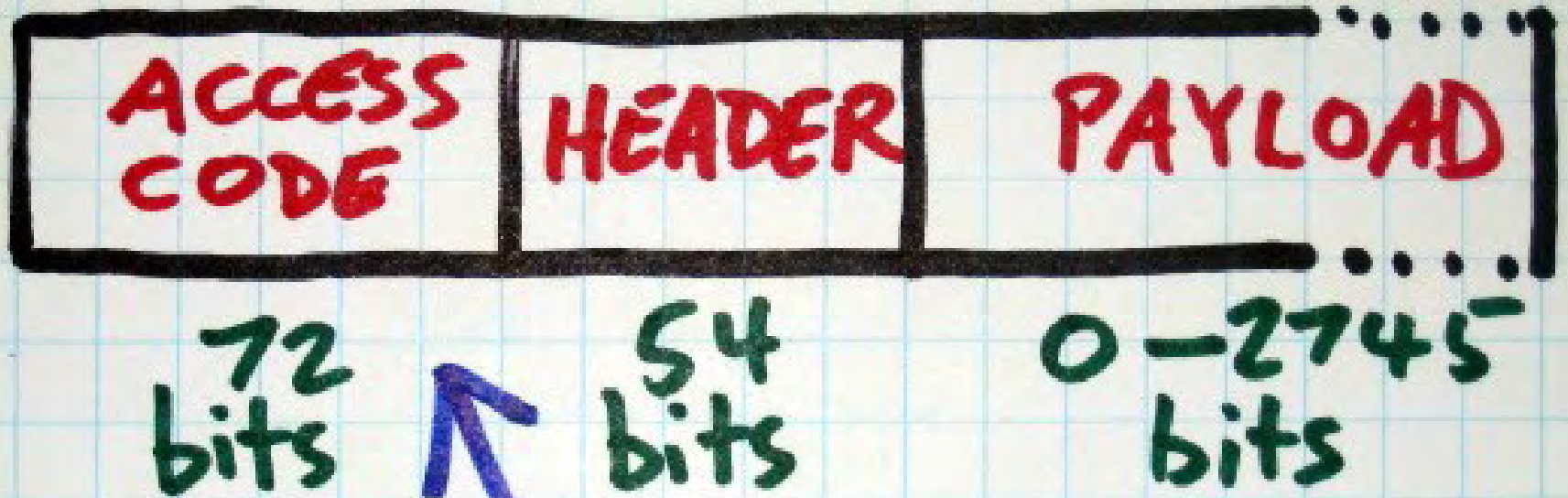
Sniffing a single channel

how?



demodulate in software

Woo Packets!

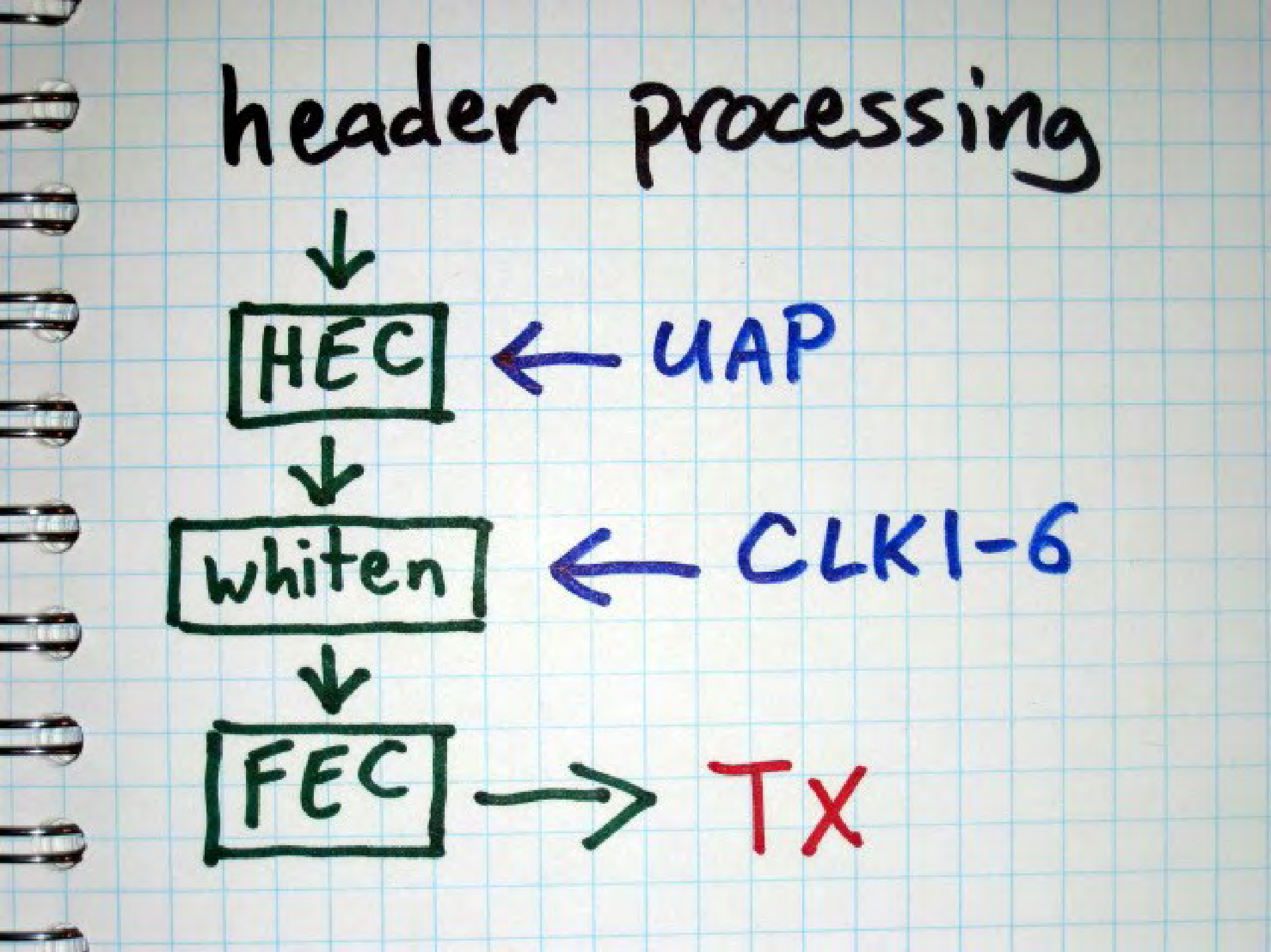

ACCESS CODE
HEADER
PAYLOAD
72 bits
54 bits
0–2745 bits
includes LAP

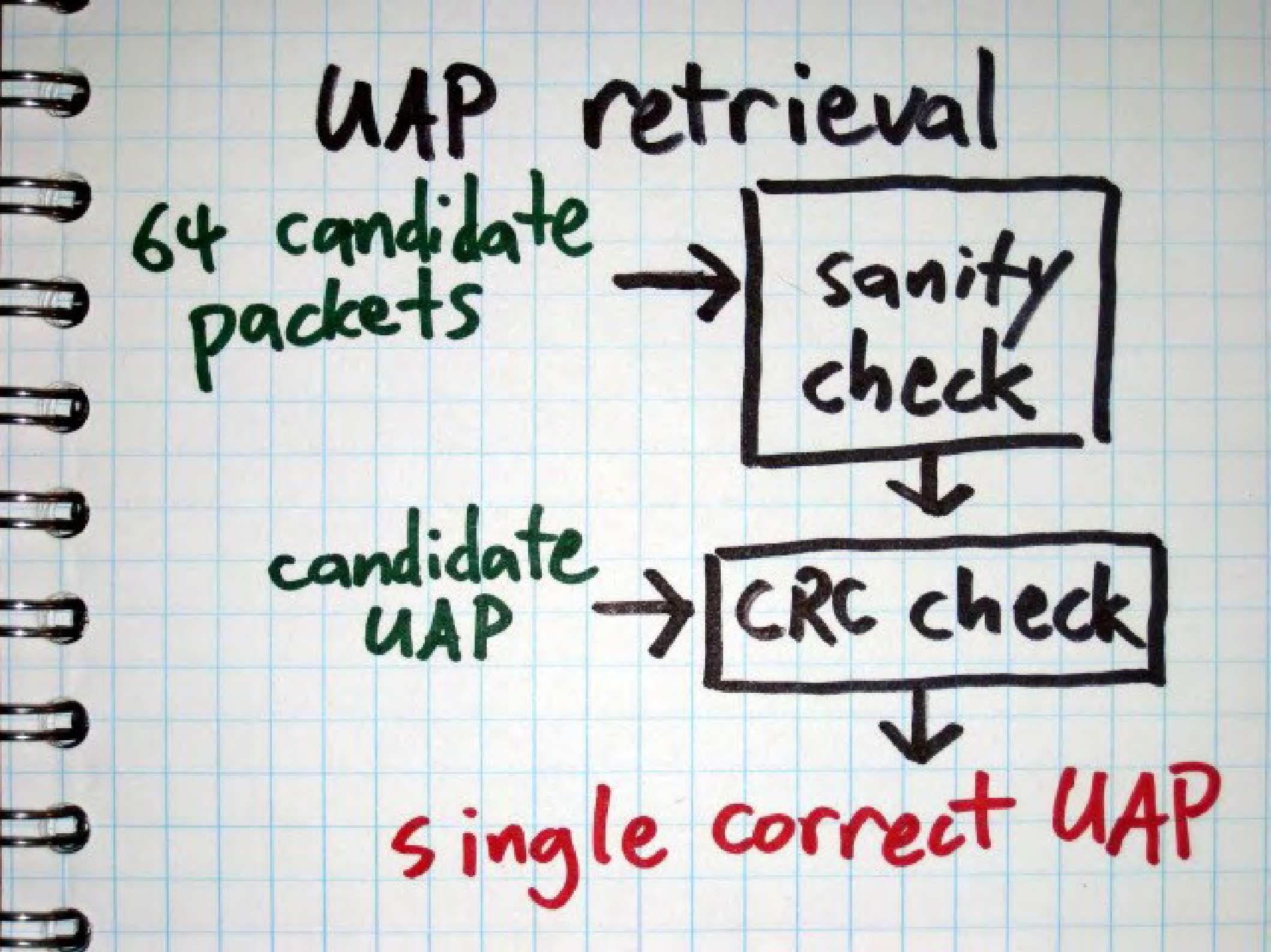
UAP discovery

not as simple as LAP

not transmitted in the clear

used for error checking


header processing
HEC
UAP
whiten
CLK1-6
FEC
TX


UAP retrieval
64 candidate packets
sanity check
candidate UAP
CRC check
single correct UAP

demonstration

retrieving the UAP

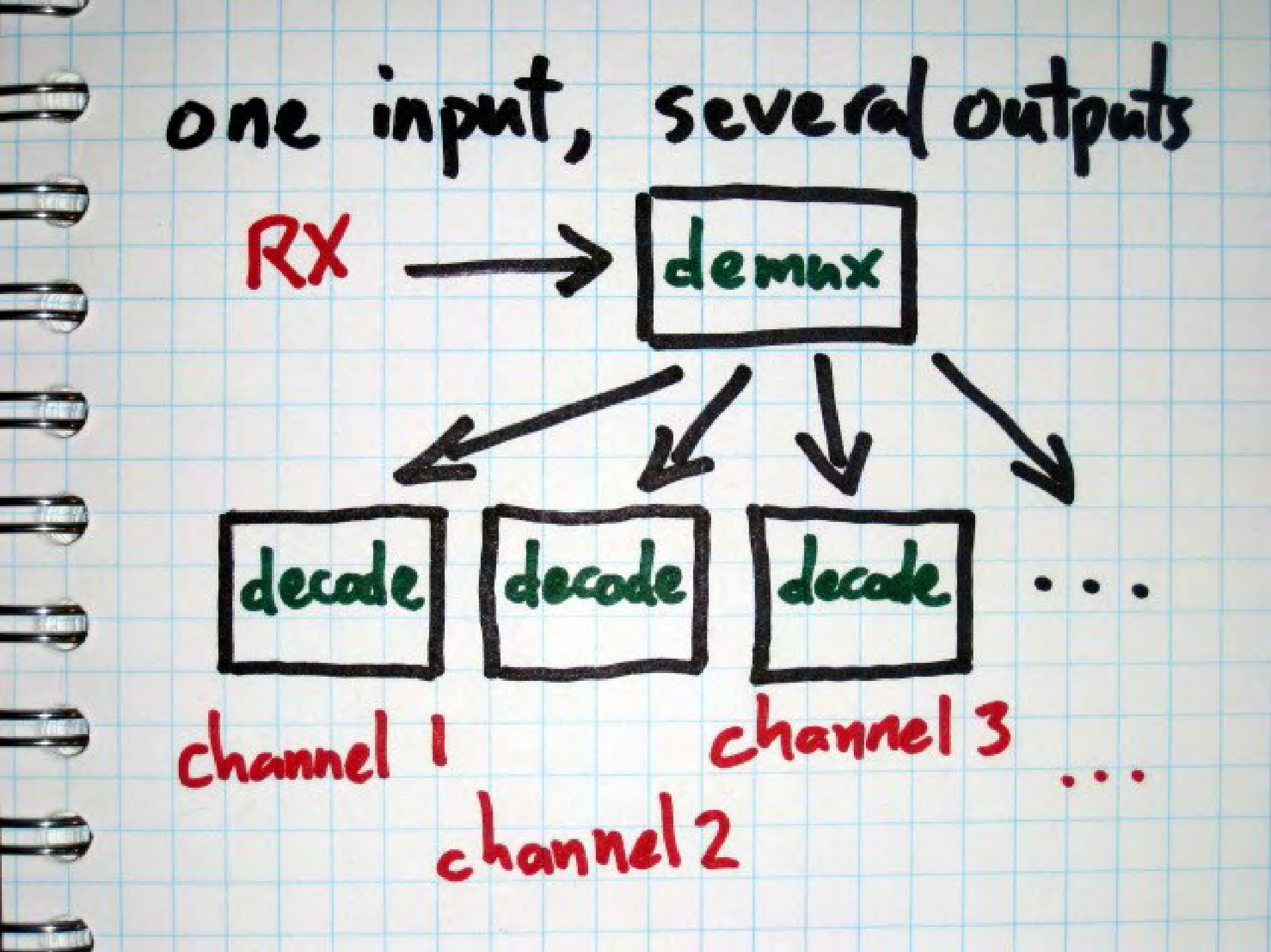
payload data

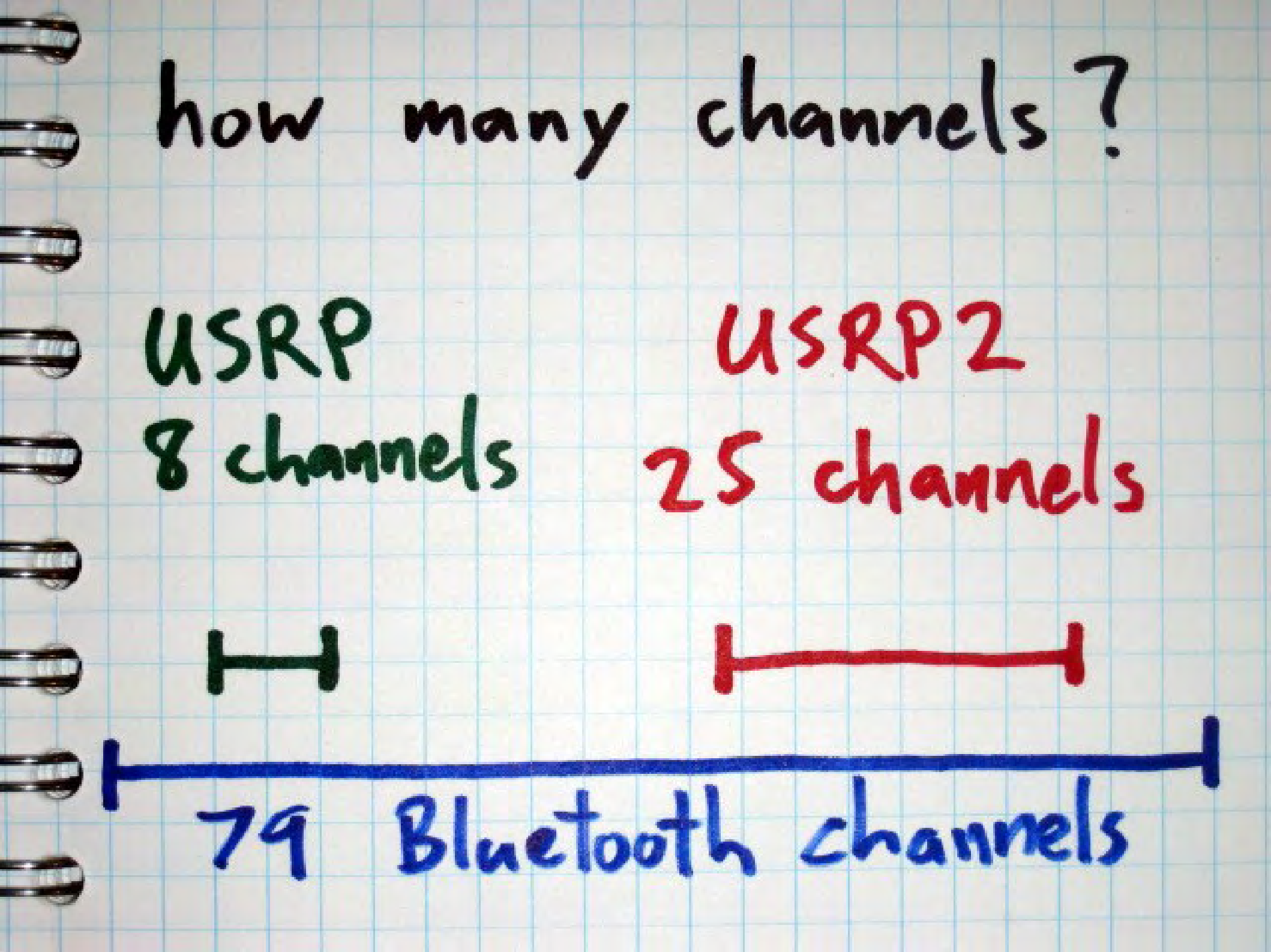
got LAP and UAP?

now we can:

- sniff packets
- verify checksums
- discover CLK1-6

Extending to Several Channels


one input, several outputs
RX
demux
decode
decode
decode
...
channel 1
channel 2
channel 3
...


how many channels ?
USRP
8 channels
USRP2
25 channels
79 Bluetooth channels

all 79 channels?

10 USRPs

or

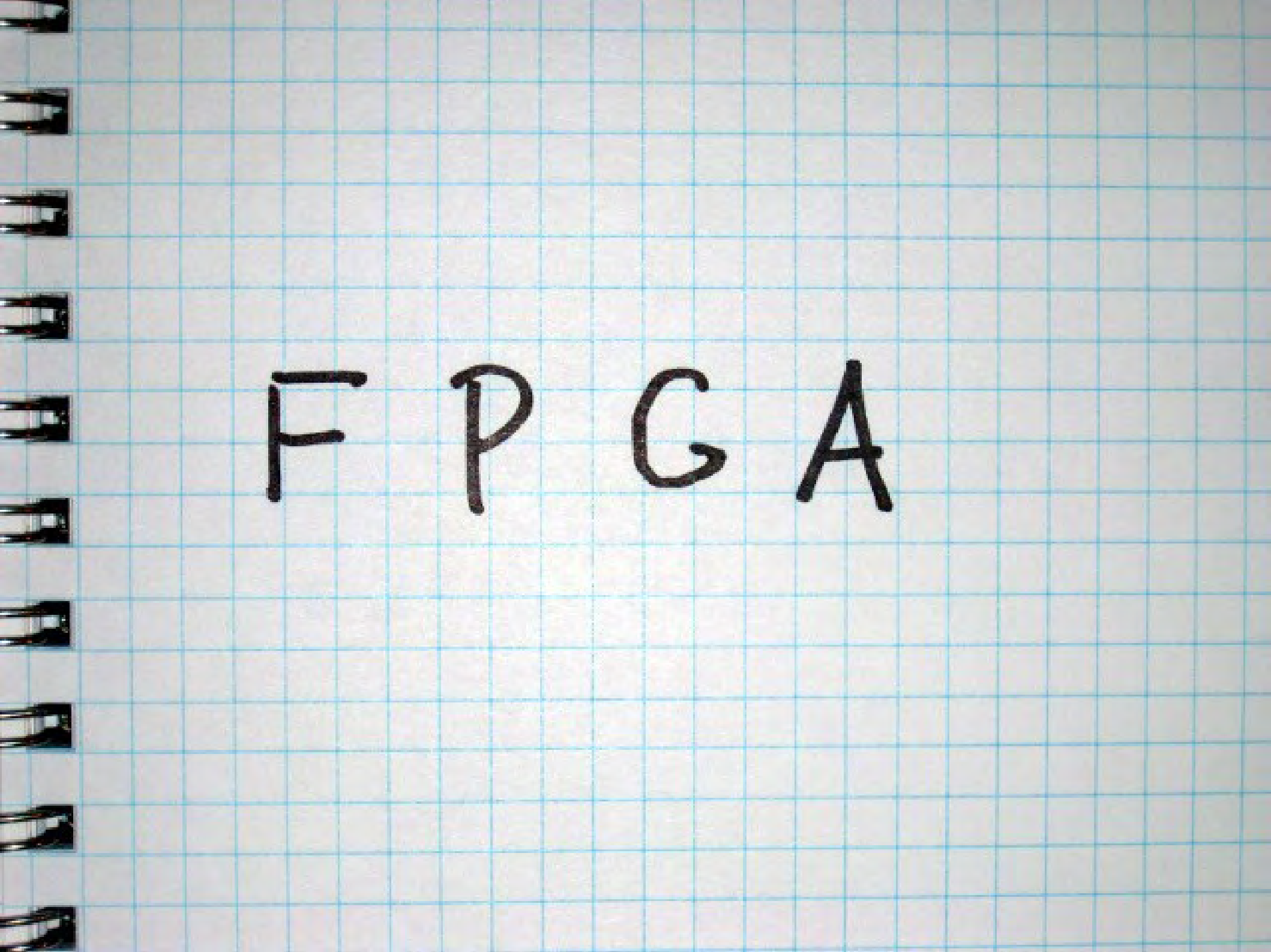
4 USRP2s



CPU requirements

1 CPU ≈ 1 channel

bus speeds,
storage,
etc.


FPGA

Predicting the Hopping Pattern

why?

sniffing all channels is too costly

active attacks

it's fun!

hopping sequence

UAP
0x65

LAP
0x87CBA9

clock	channel
0	20
2	60
4	53
6	62
⋮	⋮

how?

use algorithm in spec

requires LAP, UAP, clock

generate entire pattern

for all clock values (~24hr)

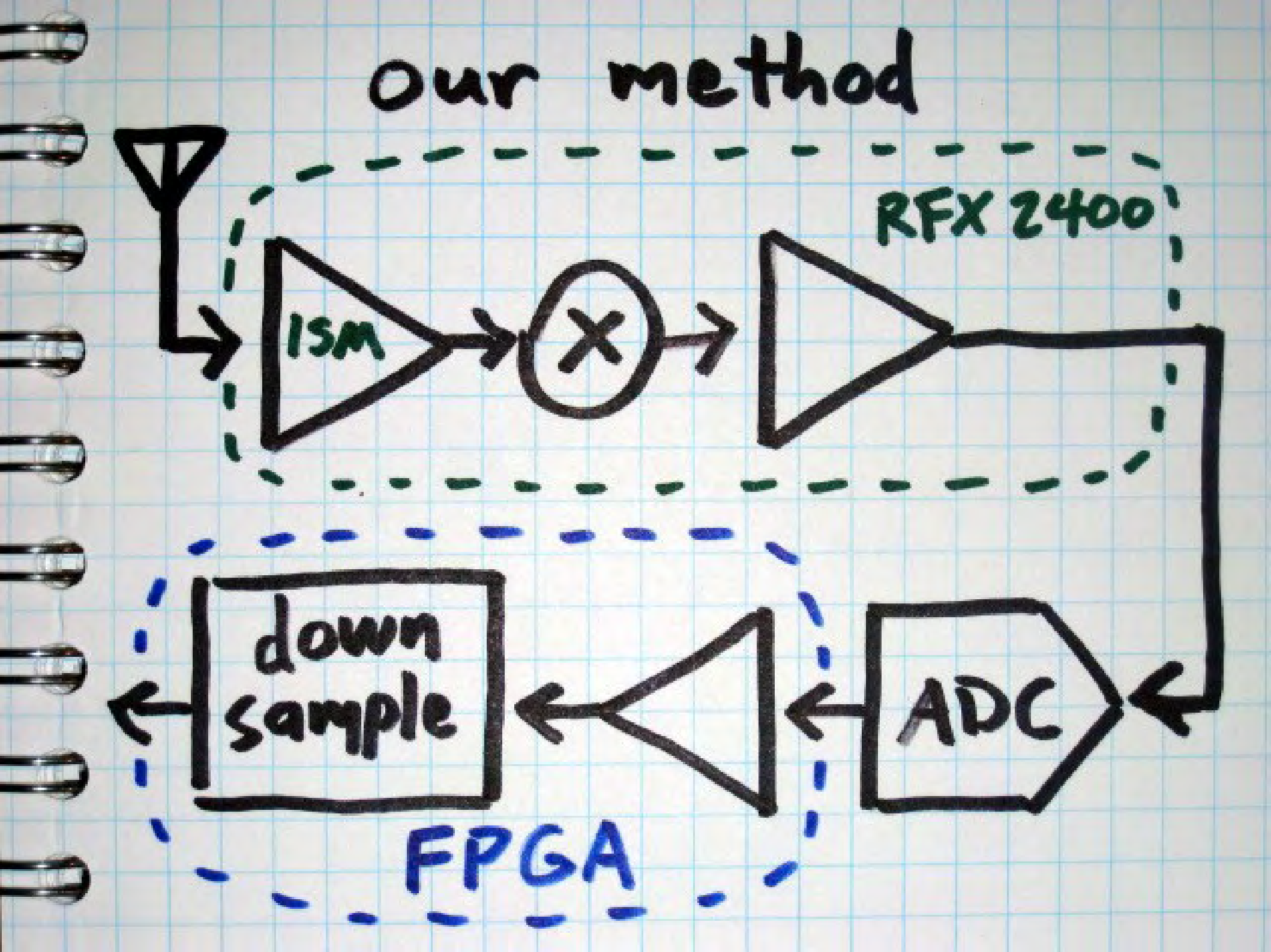
search the pattern

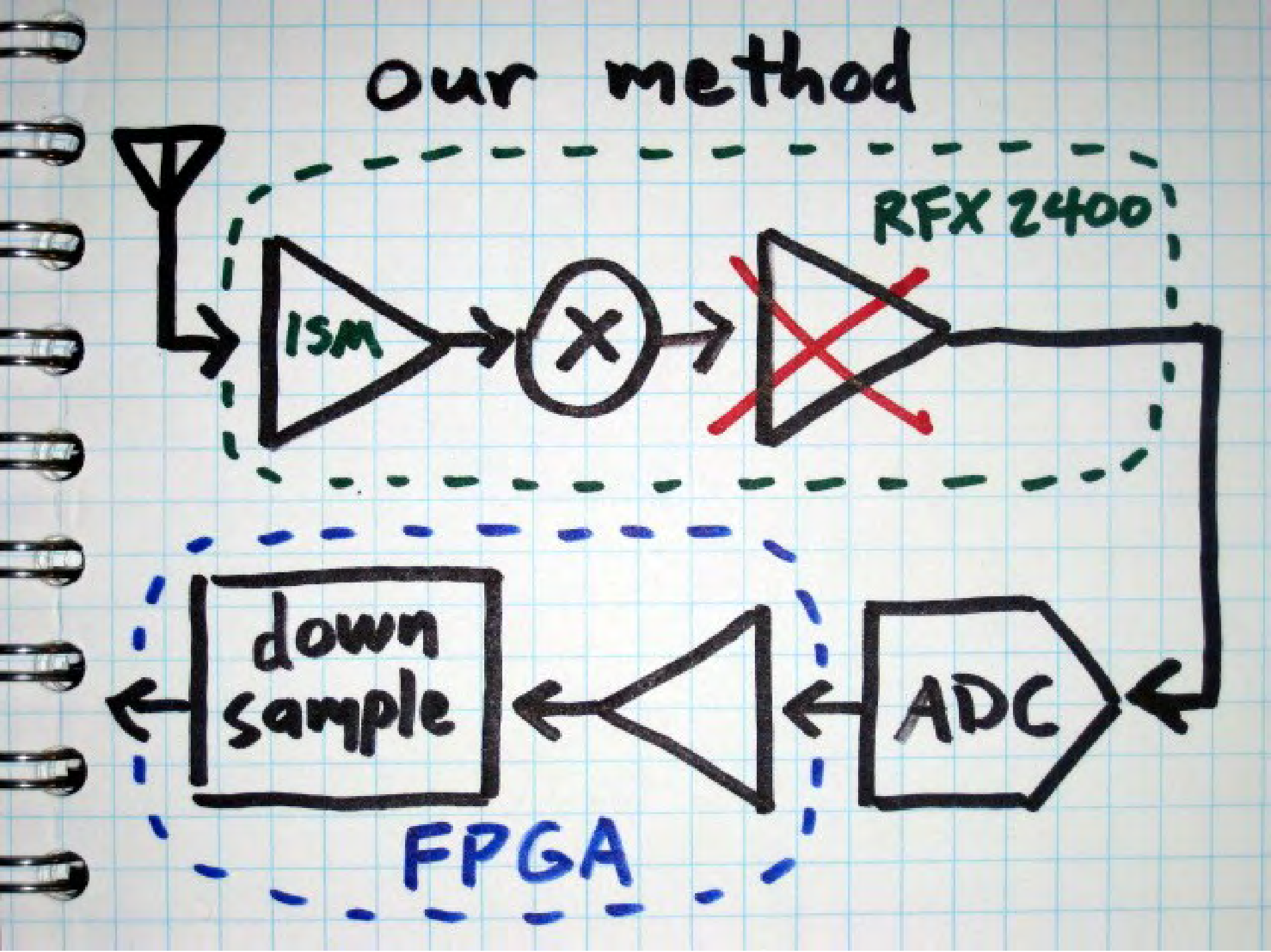
using observed hops

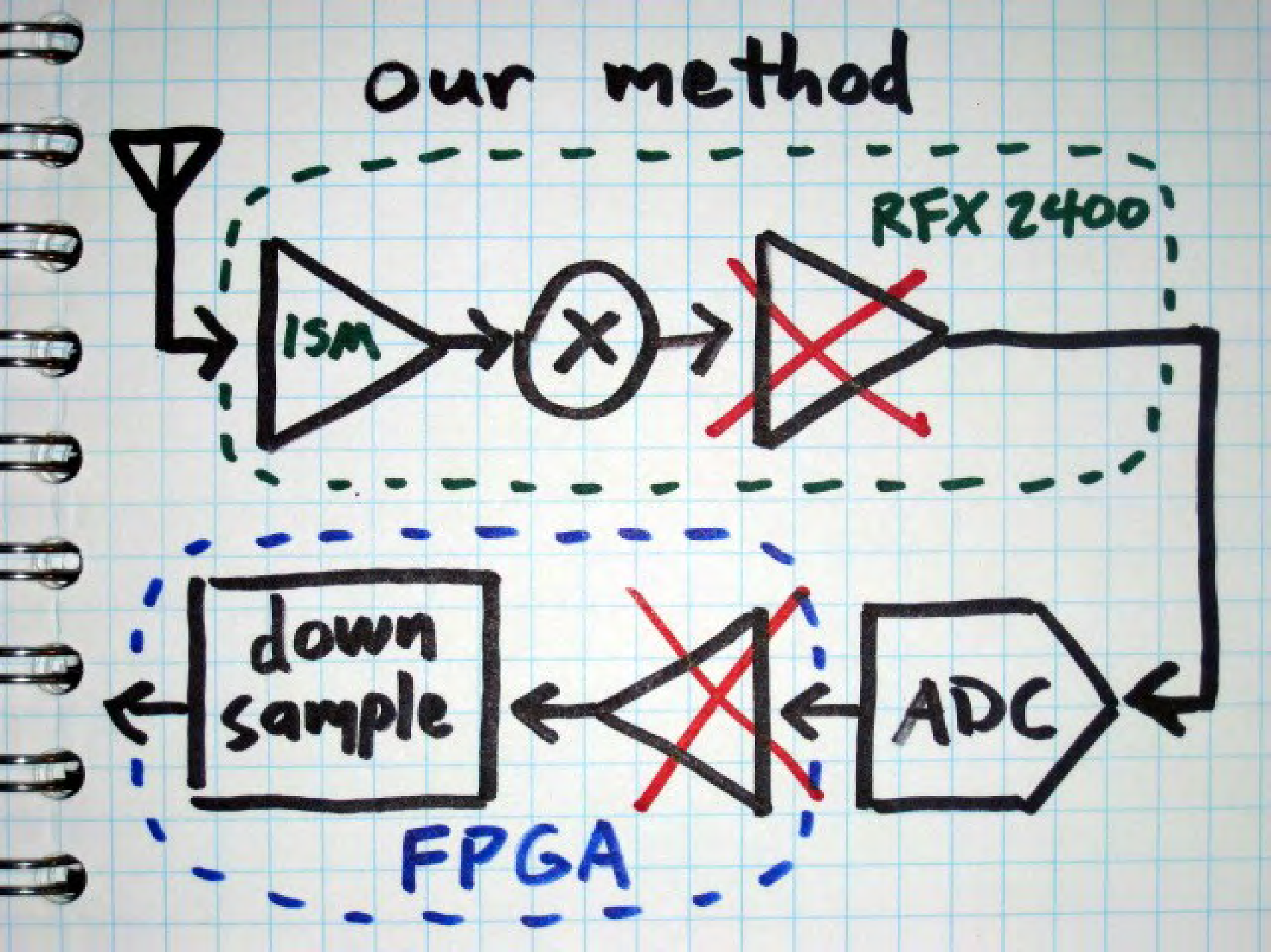
demonstration

finding the clock

Intentional Aliasing


our method
RFX 2400
ISM
down sample
ADC
FPGA


our method
RFX 2400
ISM
down sample
ADC
FPGA


our method
RFX 2400
ISM
down sample
ADC
FPGA

demonstration

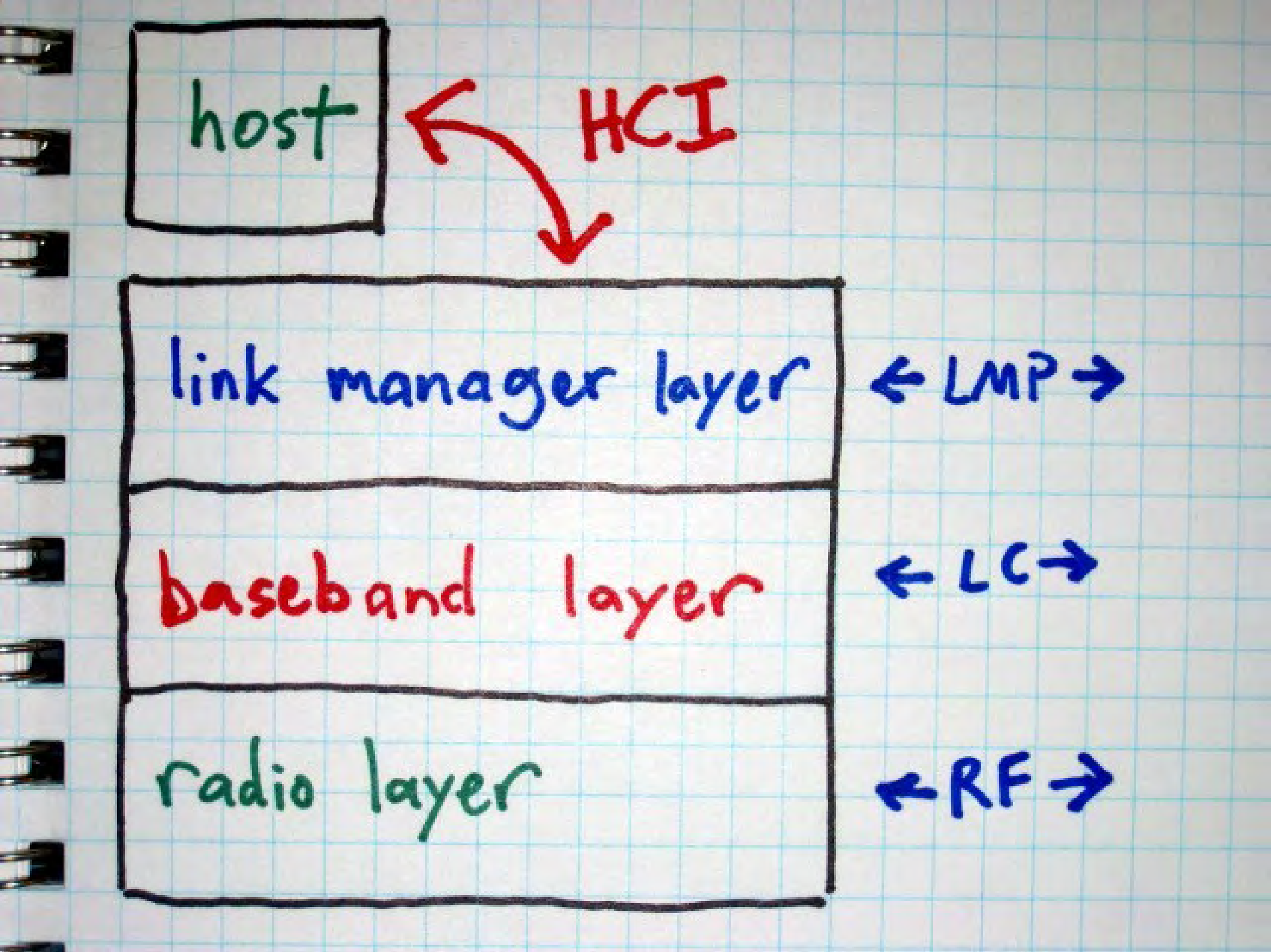
aliased
hopping

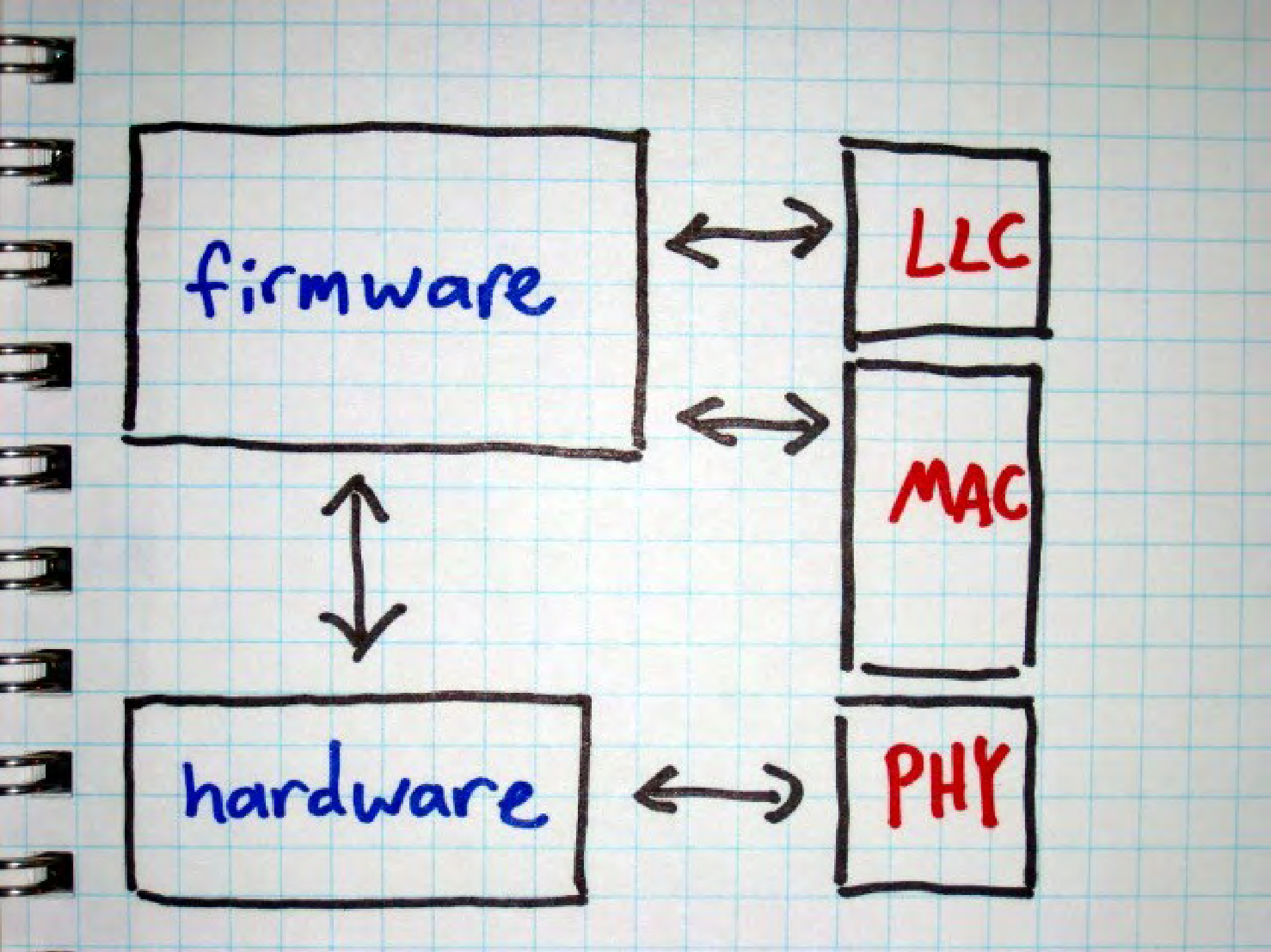

Bluetap

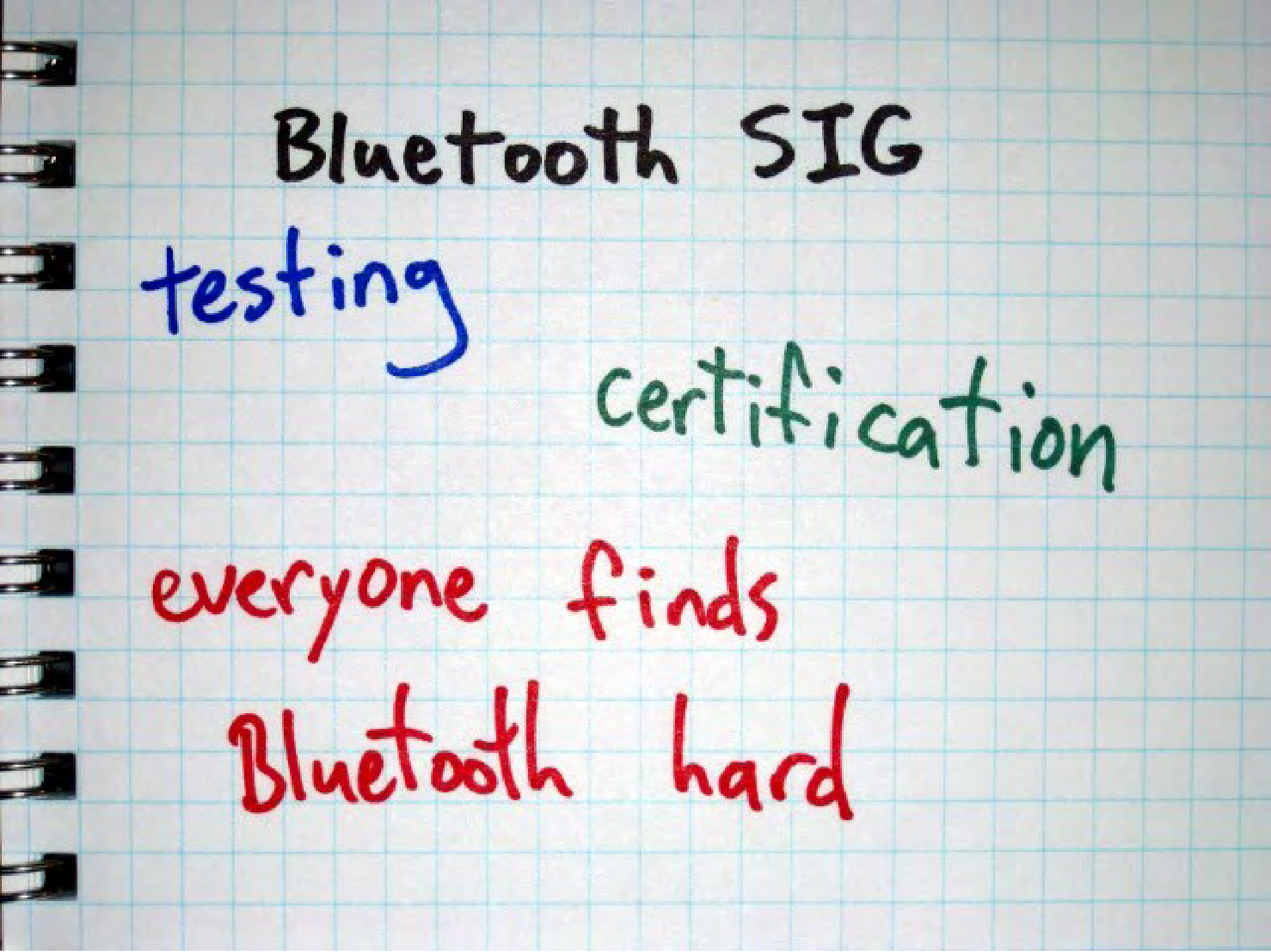
a different attack

2 billion
Bluetooth devices

surely one of them
is programmable?


host
HCI
link manager layer
LMP
baseband layer
LC
radio layer
RF


firmware
LLC
MAC
hardware
PHY

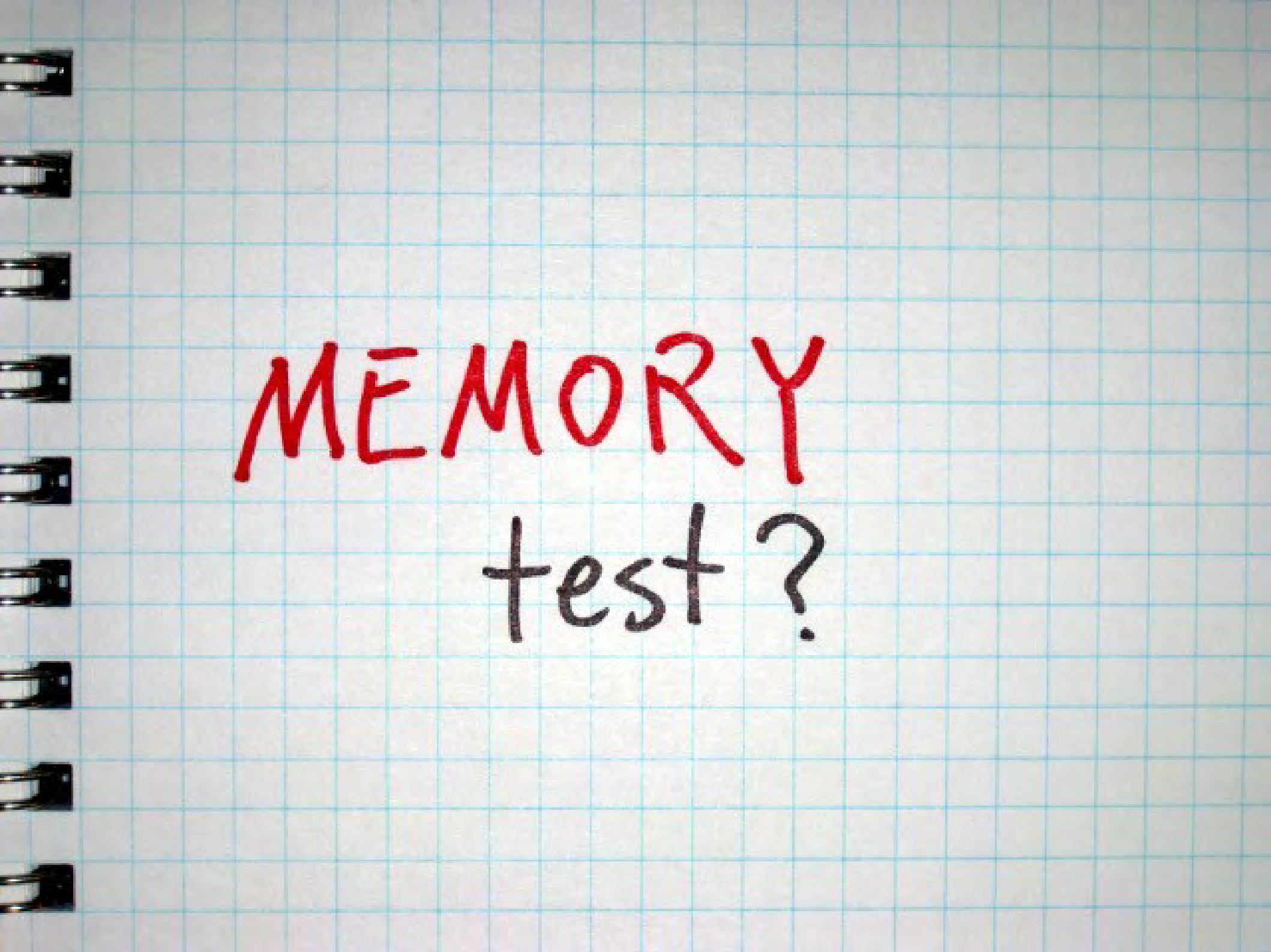

Bluetooth SIG
testing
certification
everyone finds
Bluetooth hard

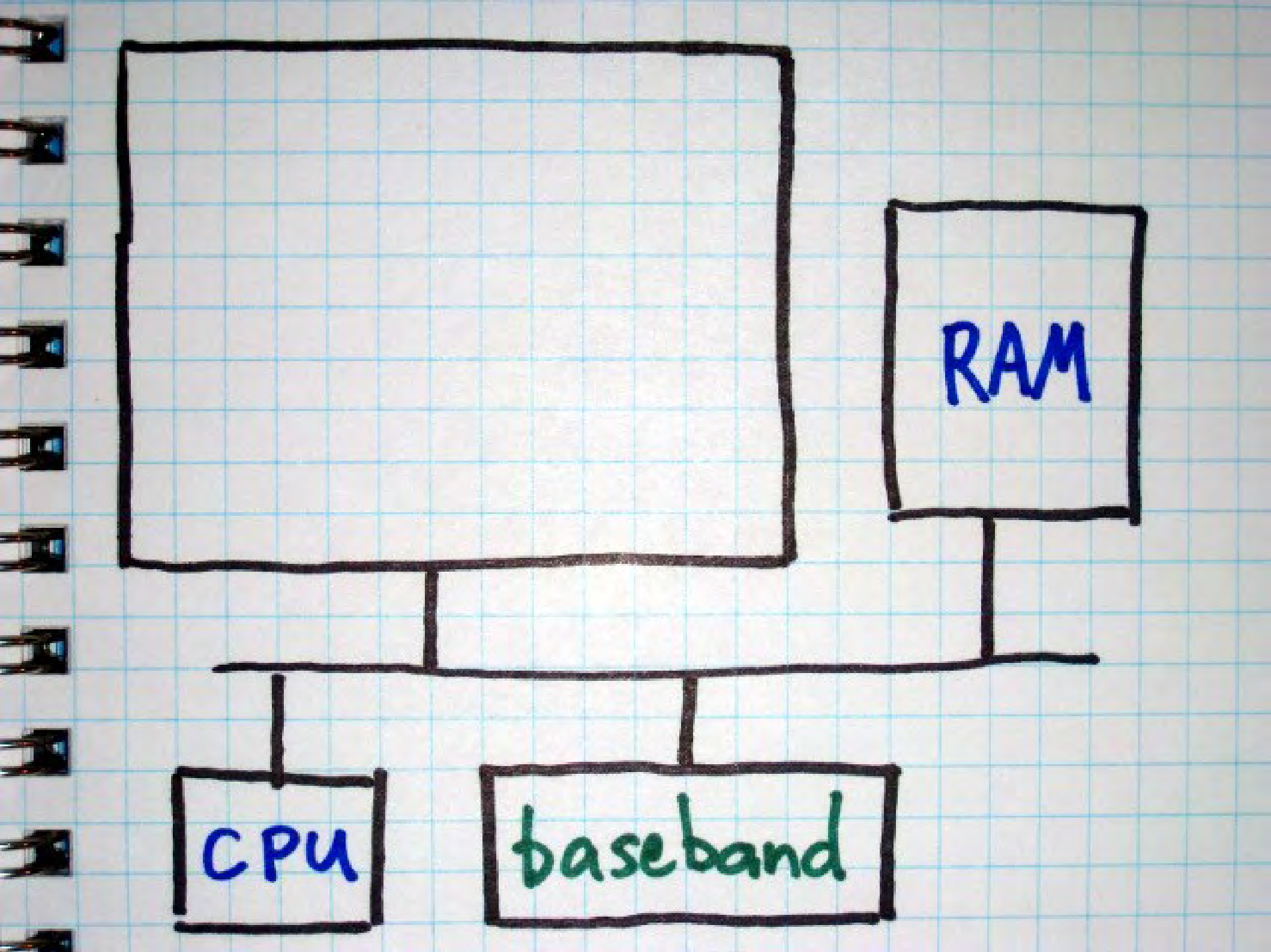
test interfaces

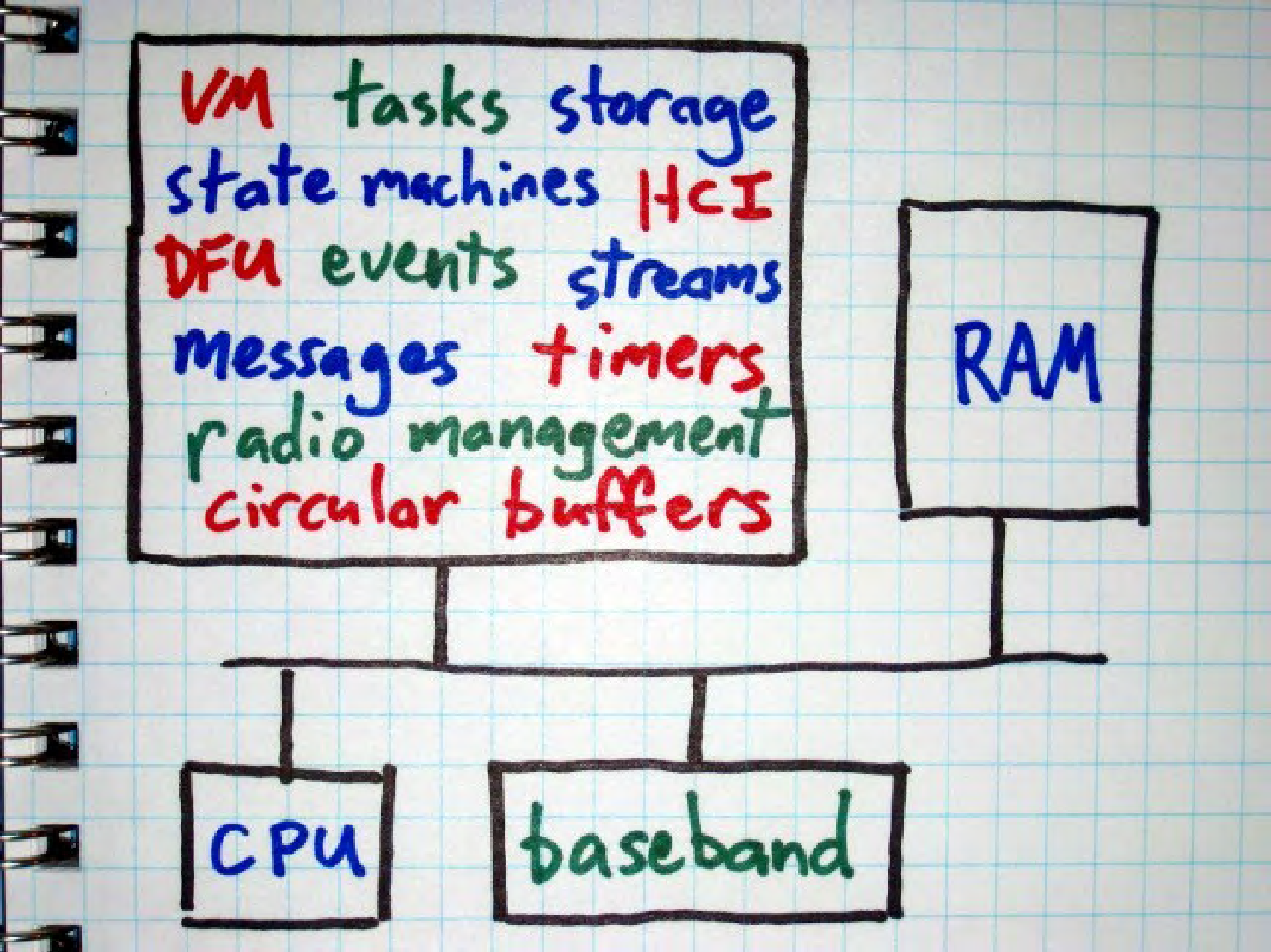
additional modules for test

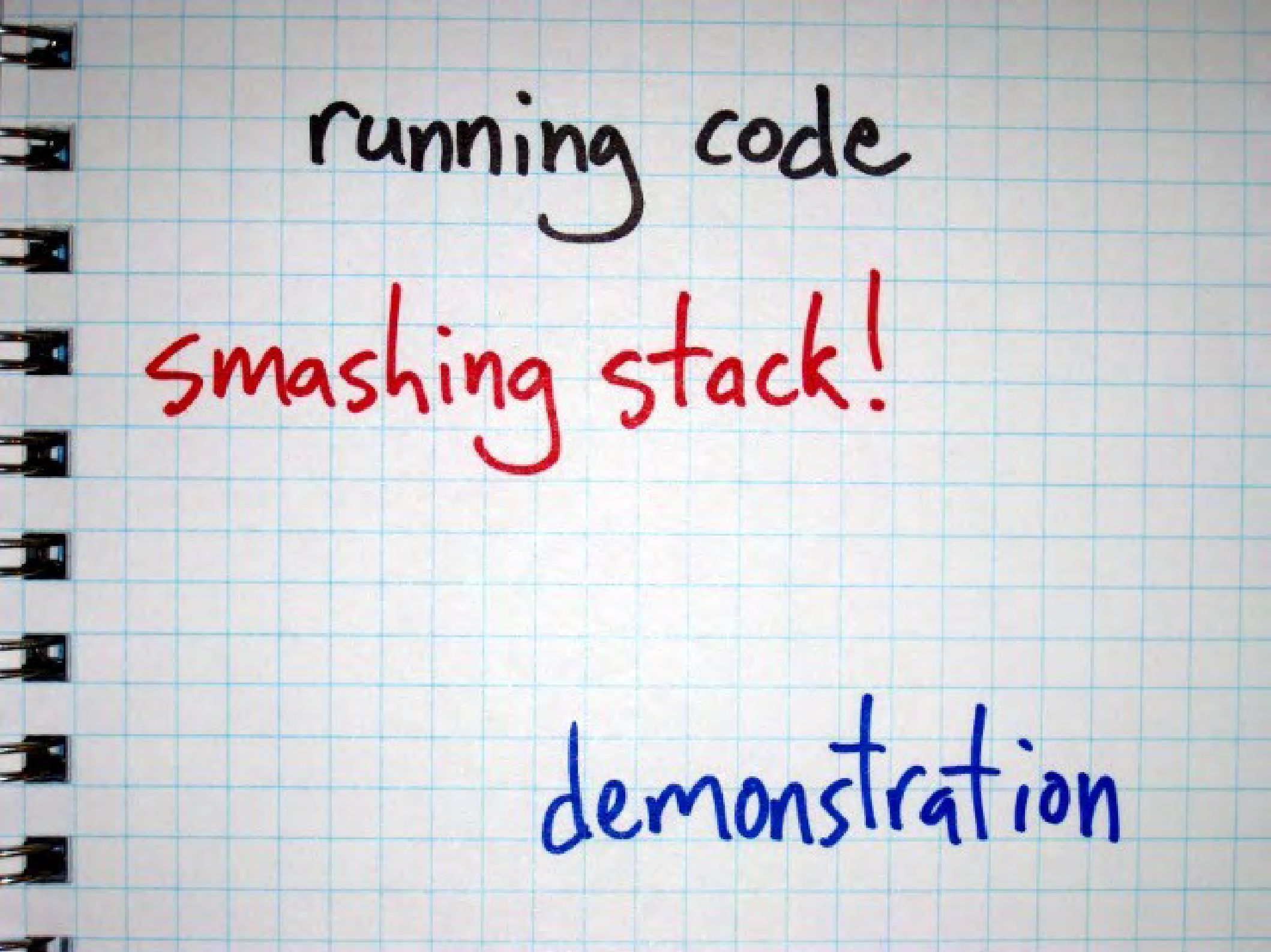
firmware is bigger

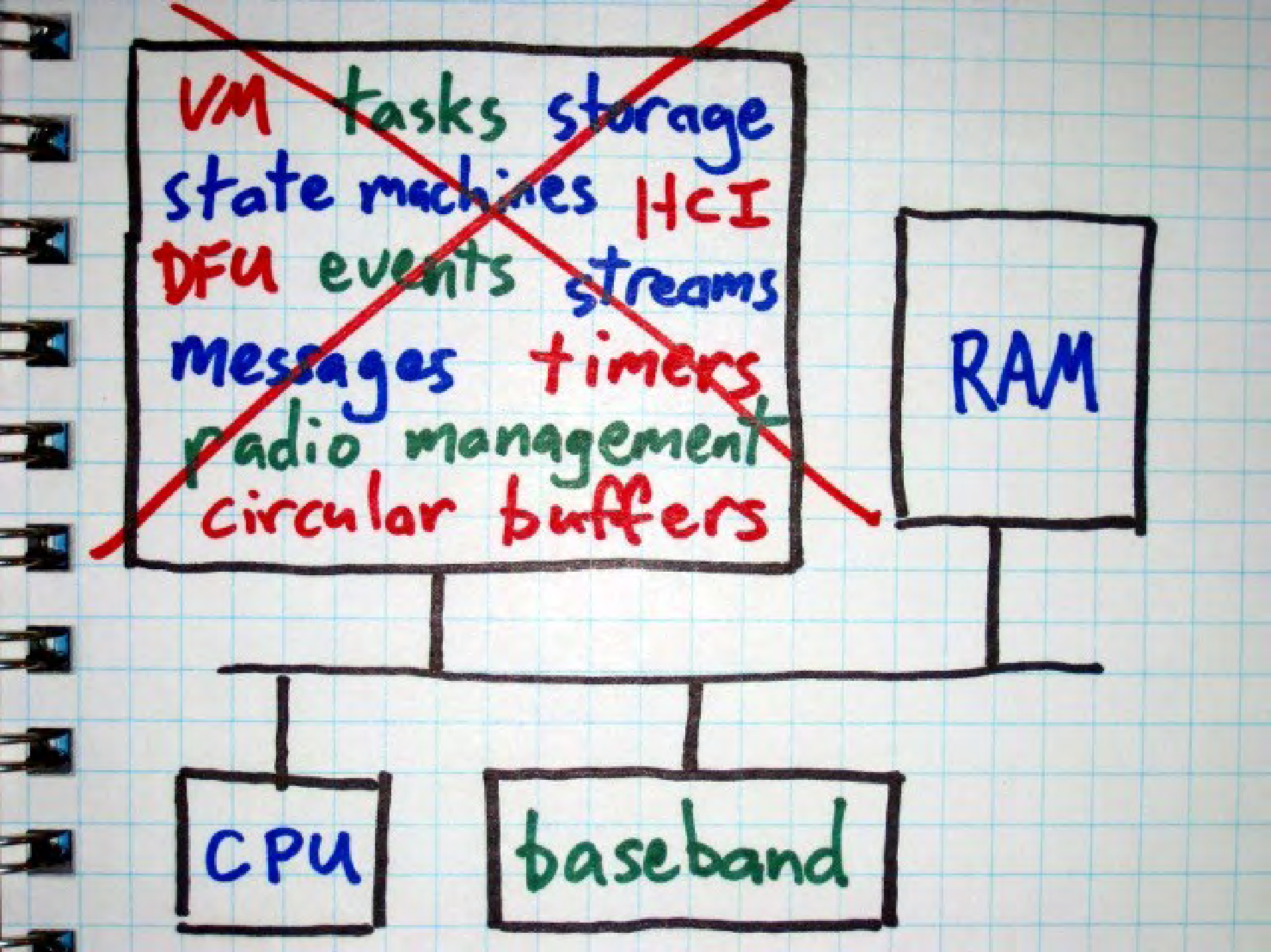
understanding it is much simpler

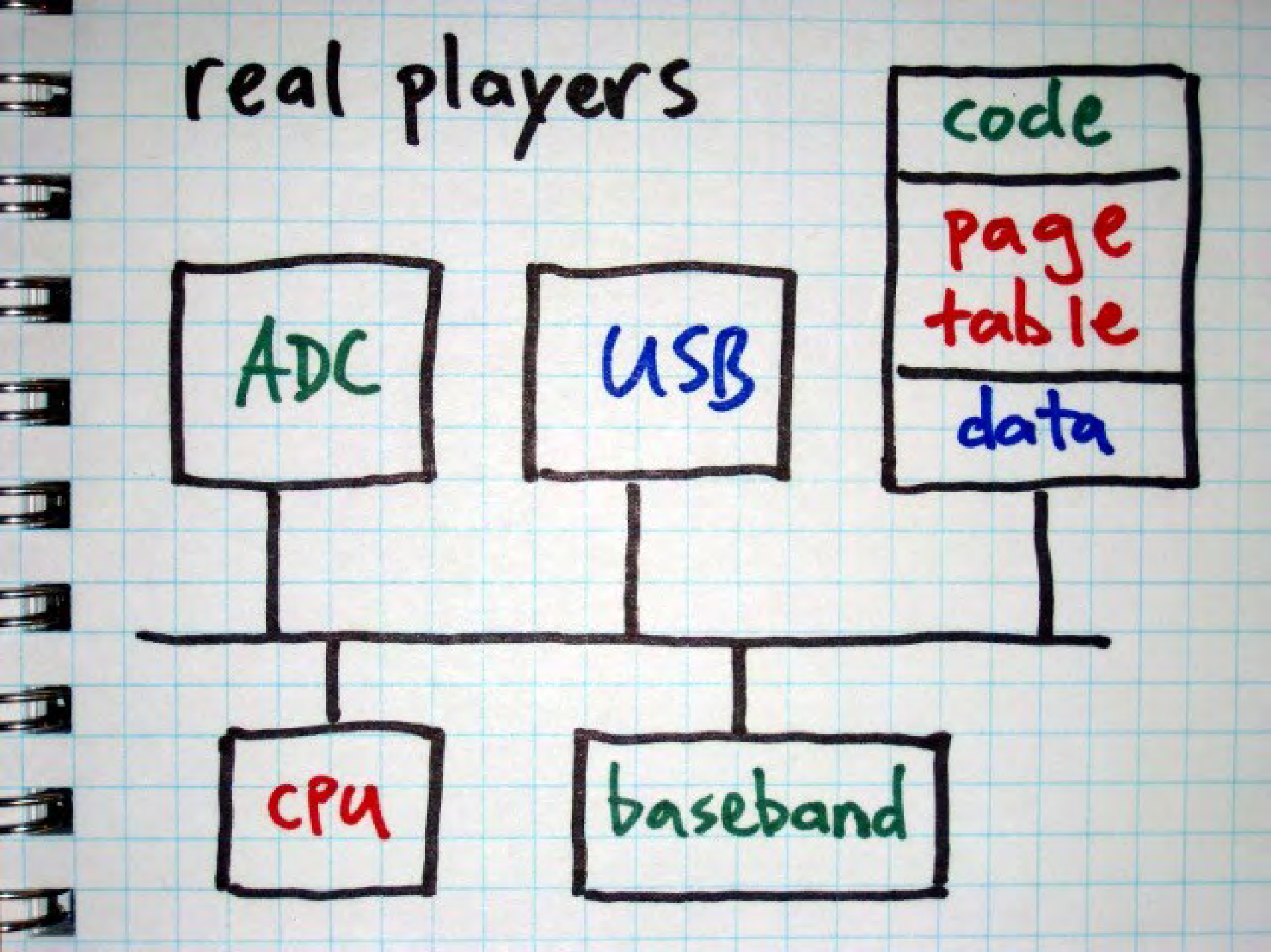

MEMORY
test ?


RAM
CPU
baseband


VM tasks storage
state machines HCI
DFU events streams
messages timers
radio management
circular buffers
RAM
CPU
baseband


running code
smashing stack!
demonstration

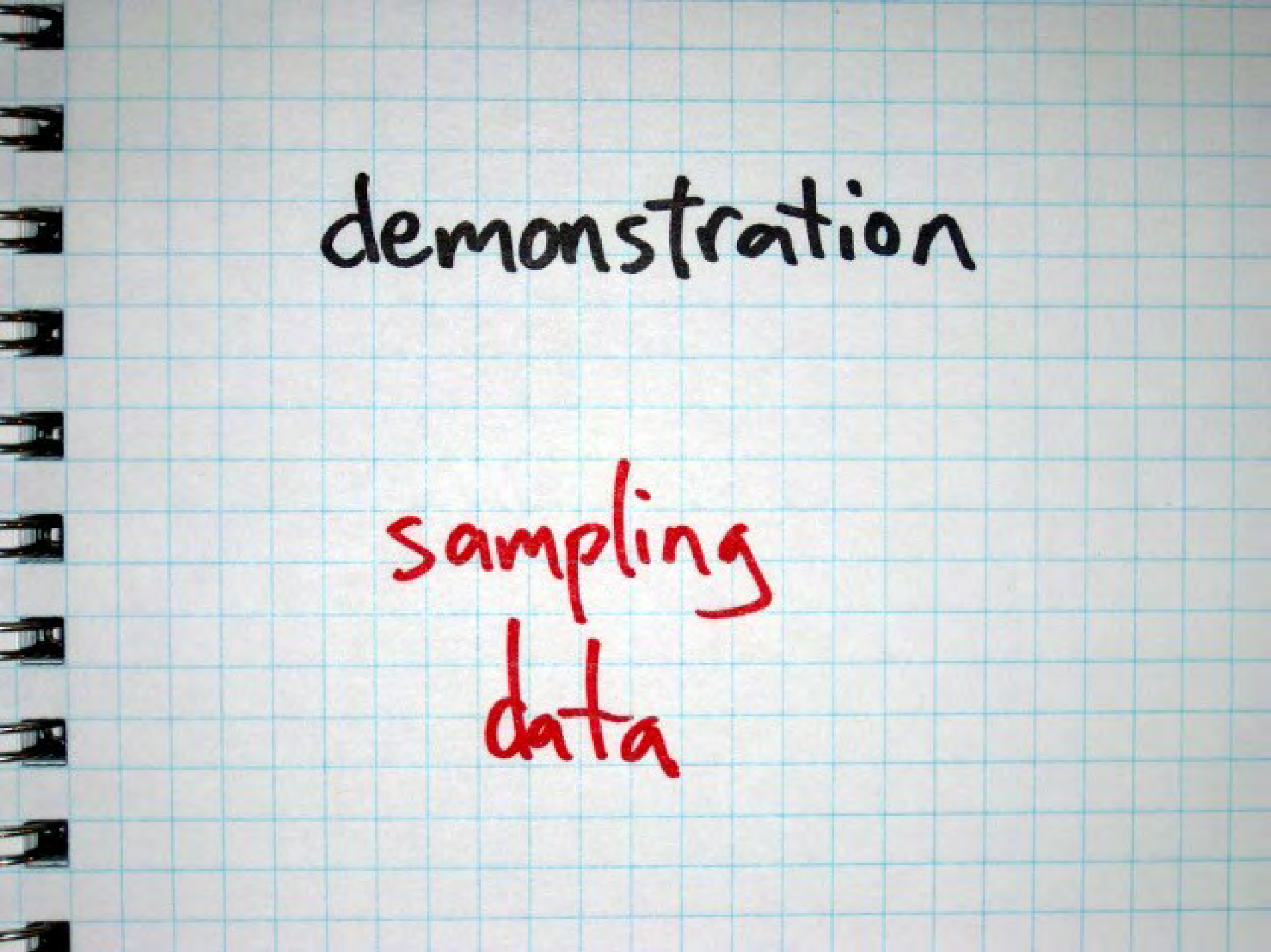

VM
tasks
storage
state machines
HCI
DFU
events
streams
messages
timers
radio management
circular buffers
RAM
CPU
baseband


real players
code
page table
data
ADC
USB
CPU
baseband

timing problems

not much time for bit bashing

MMU is a nuisance


demonstration
sampling
data

demonstration

injecting data

multiple channels

Much easier -

multiple devices

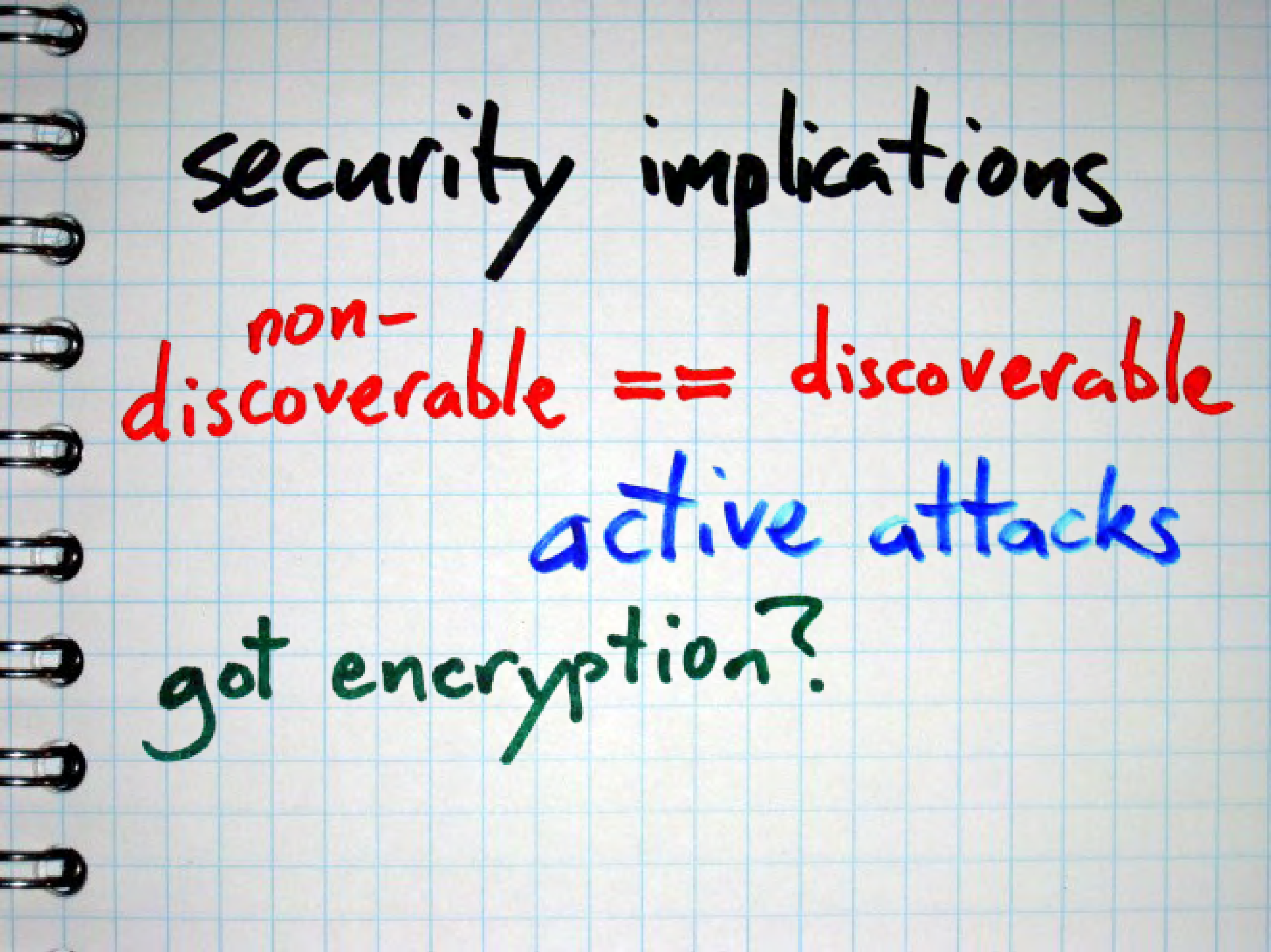
randomness helps

bluetap

open source release

links with gr-bluetooth

bluetap.org


security implications
non-discoverable == discoverable
active attacks
got encryption?

Q&A

http://gr-bluetooth.sf.net/

http://bluetap.org/