

HackRF

A Low Cost Software Defined Radio Platform



Hackito Ergo Sum 2013

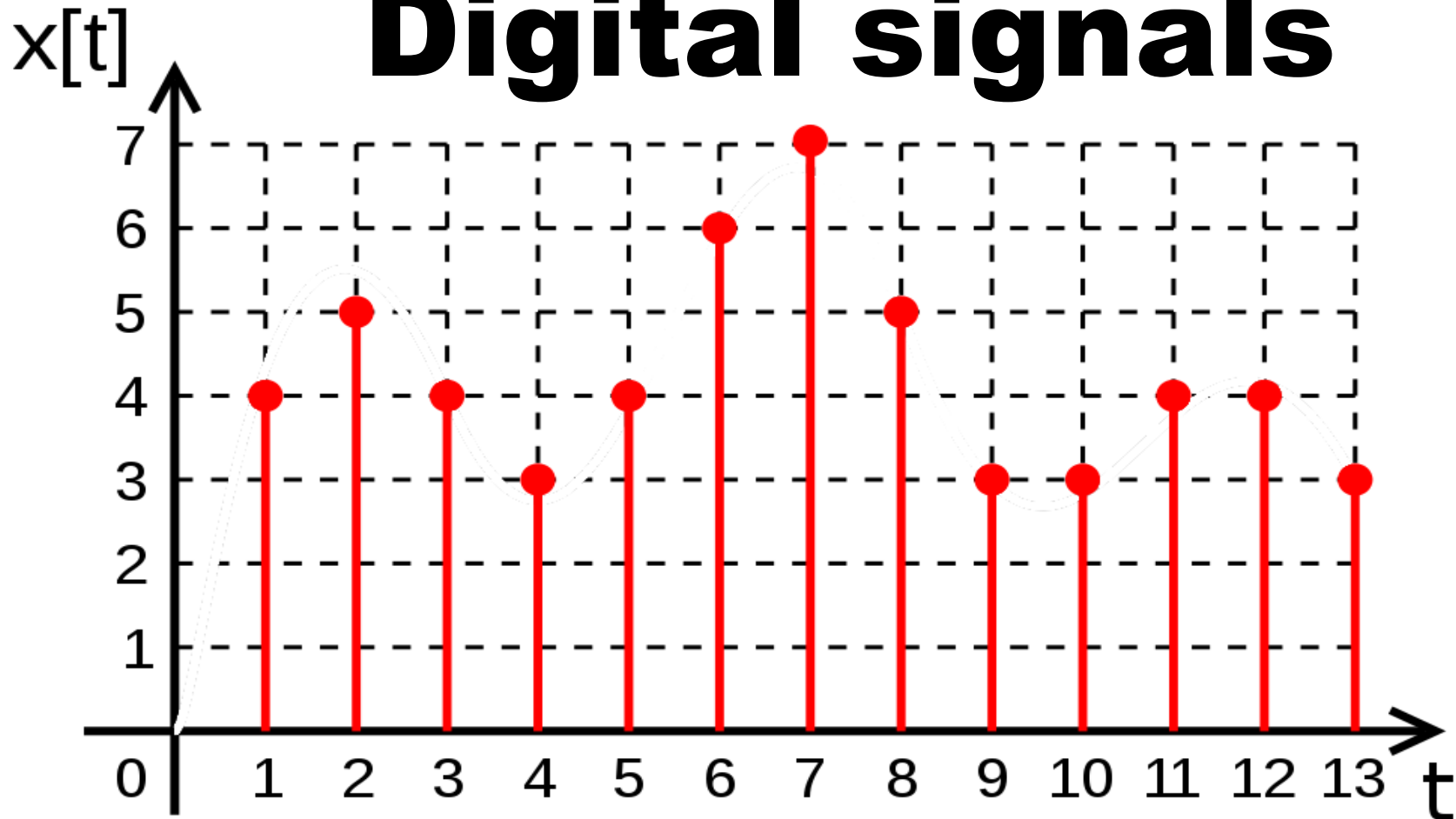
**Benjamin
Vernoux**

**Youssef
Touil**

Software Defined Radio (SDR)

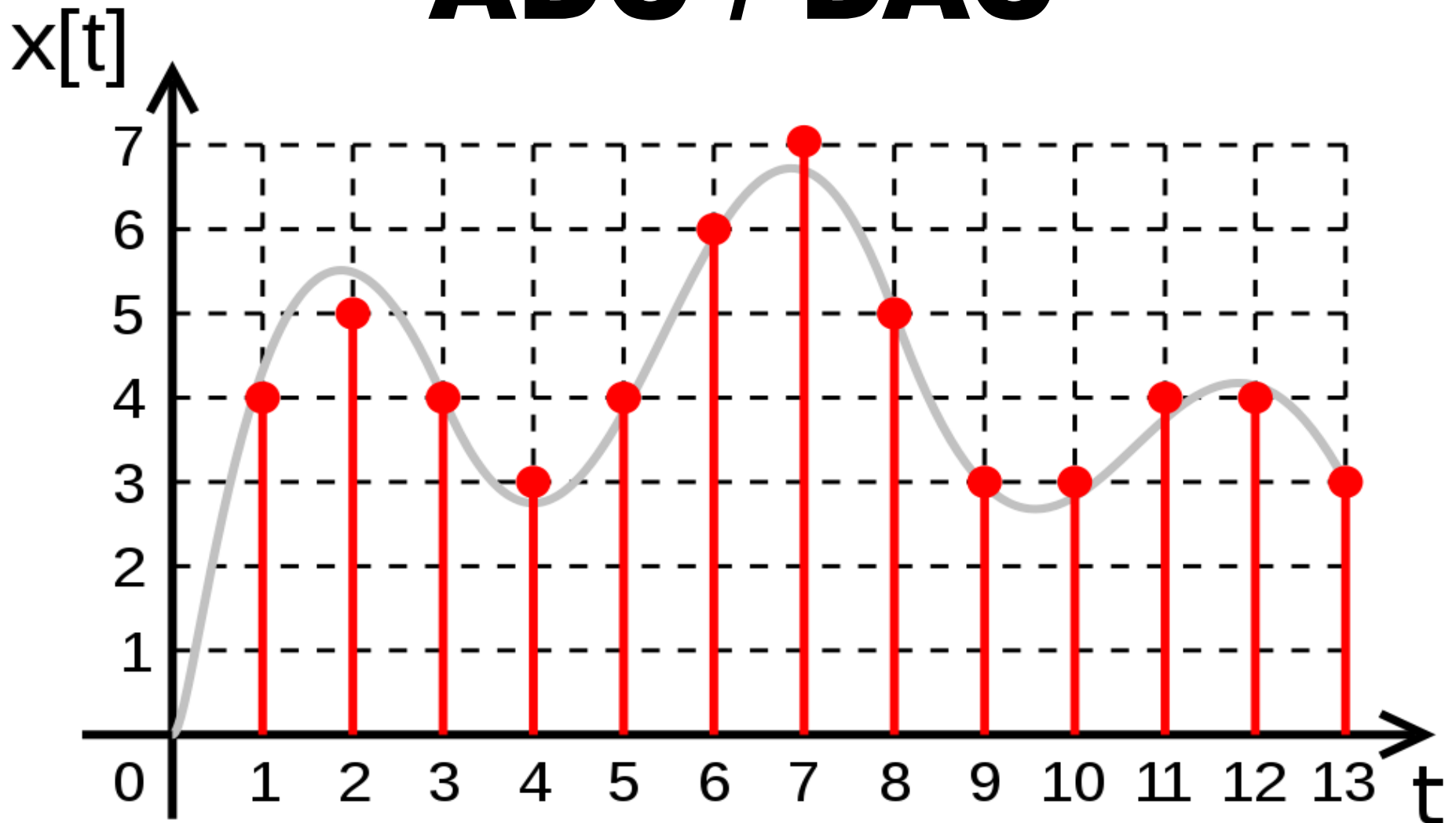
**Radio by
Digital Signal Processing
(DSP)**

Digital signals



A digital signal is a physical signal that is a representation of a sequence of discrete values like a digitized analog signal.

ADC / DAC



<http://upload.wikimedia.org/wikipedia/commons/0/04/Digital.signal.discret.svg>

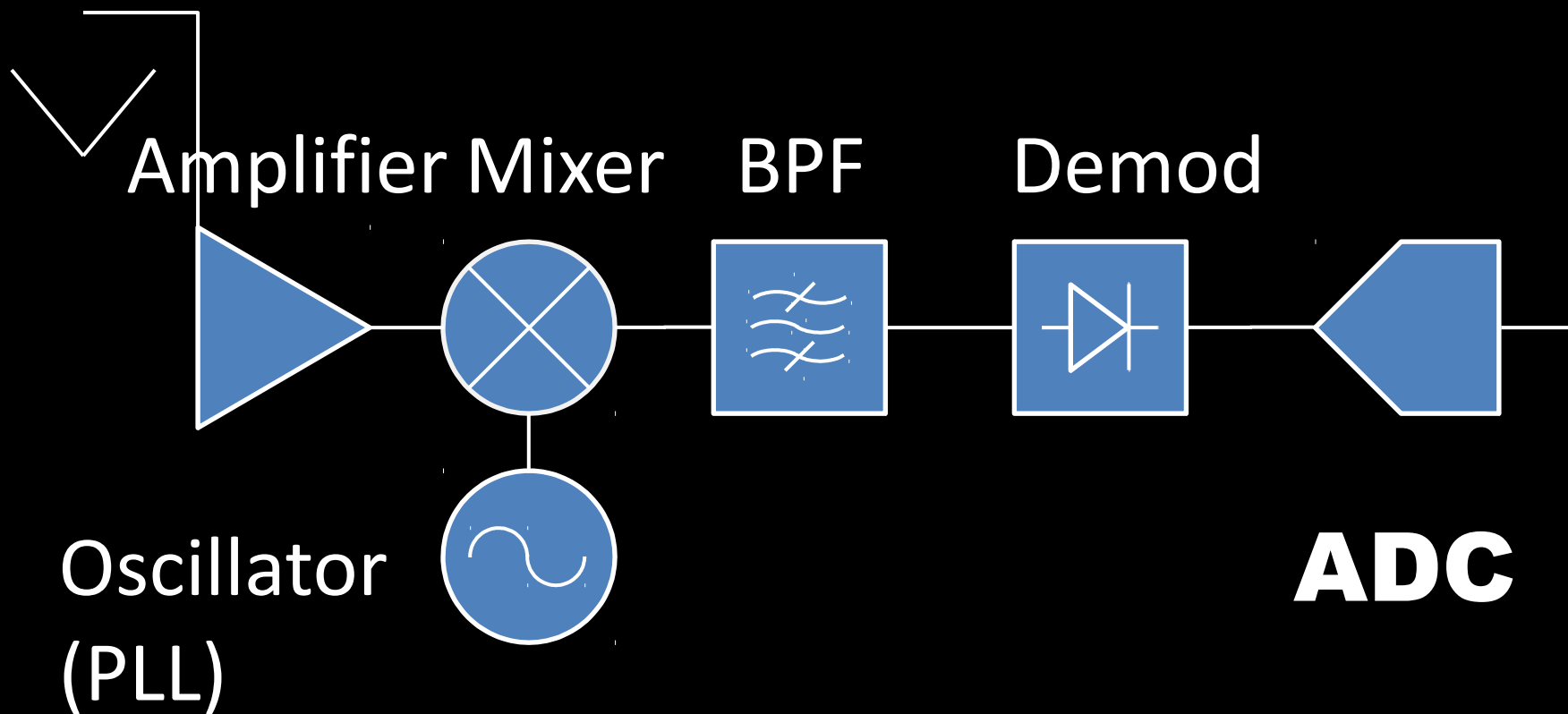
Analog Audio

- **Phonograph
(Thomas Edison 1877)**
- **Gramophone / Vinyl records**
- **Magnetophon / Tape**
- **Old Telephone**

Digital Audio

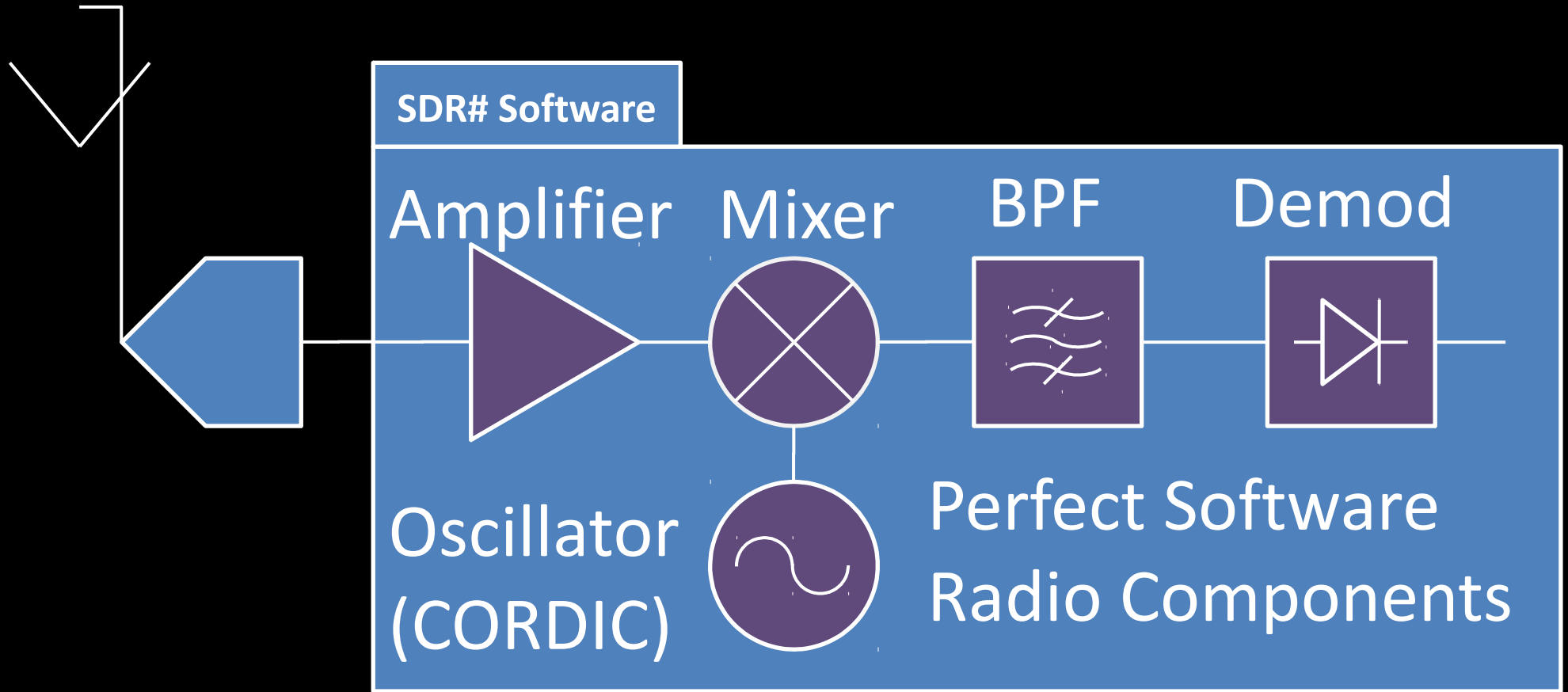
- **DECT (Phone)**
- **CD/DVD/Blu-Ray**
- **DAT**
- **Hard Disk Recorder**

The world of analog radio...



Synopsis of a single conversion
radio

The Software Defined Radio



Synopsis of a radio implemented by software components

Fexibility

Many Radios in one

(with the right

antenna)

Right Antenna

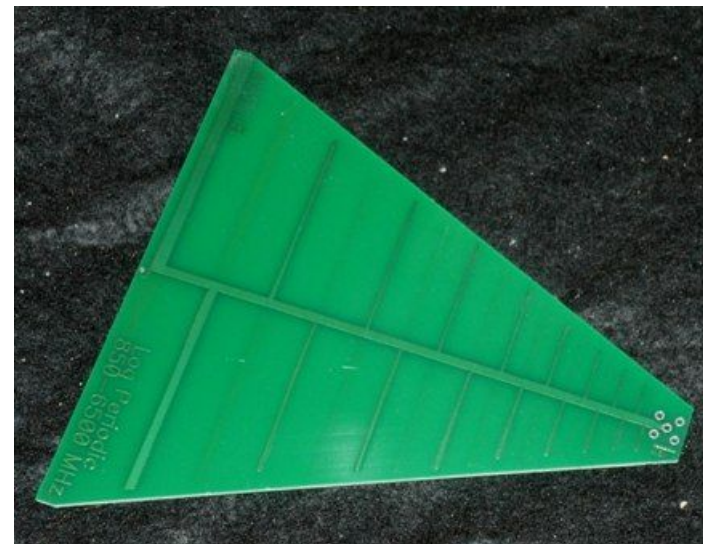
like cheap (less than 30USD)

Log Periodic PCB Antennas



400 to 1000

MHz



850 to 6500

MHz

<http://www.wa5vjb.com/products1.html>

Reconfigurability

Software Modification

The Future

All radios

will be software

radios

Target Operating Frequencies

- **0 - 1 GHz : NFC, CB/FM radio, Car/Door Key Fob, TI CC subGHz ...**
- **1 - 2 GHz: DECT, GPS, GSM**
- **2.4 GHz: 802.11, Bluetooth, Zigbee**
- **5.9 GHz: DSRC, WAVE, 802.11**

Target Bandwidth

- **0 - 1 MHz : Lot of stuff**
- **1 MHz: Bluetooth**
- **2 MHz: Zigbee, DECT**
- **5 MHz: LTE**
- **20MHz: 802.11/WLAN**

ISM band for unlicensed use

Frequency range		Bandwidth	Center frequency
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz
433.050 MHz	434.790 MHz	1.84 MHz	433.920 MHz
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz

Respect laws of your country regarding EMI and the maximum TX power allowed per band

RECEIVE

OR

TRANSMIT

Half Duplex

(Limited by

MCU / USB 2.0HS)

We can live without

- **High dynamic range**
- **Fast DSP/FPGA**
- **Full-Duplex**

COST

**High quality
analog
components**

OR

**Cheap analog
components
+ CPU/MCU
(HackRF)**

COST

**Single device any
laptop owner can
afford.**

**For a price estimated
to 300 USD.**

**OPEN SOURCE
Hardware
and Software
(mainly GPL)**

HackRF Use Cases

- **RFID (Radio Freq Identification)**
- **Cellular GSM base station**
- **GPS receiver**
- **AM/FM Radio TX/RX, APCO-25 (USA) / TETRA (EU) Digital Radio**
- **Digital Television (ATSC/DVB-T)**
- **Passive radar**
- **And lot of others ...**

Hardware Design Process

Michael

Jared

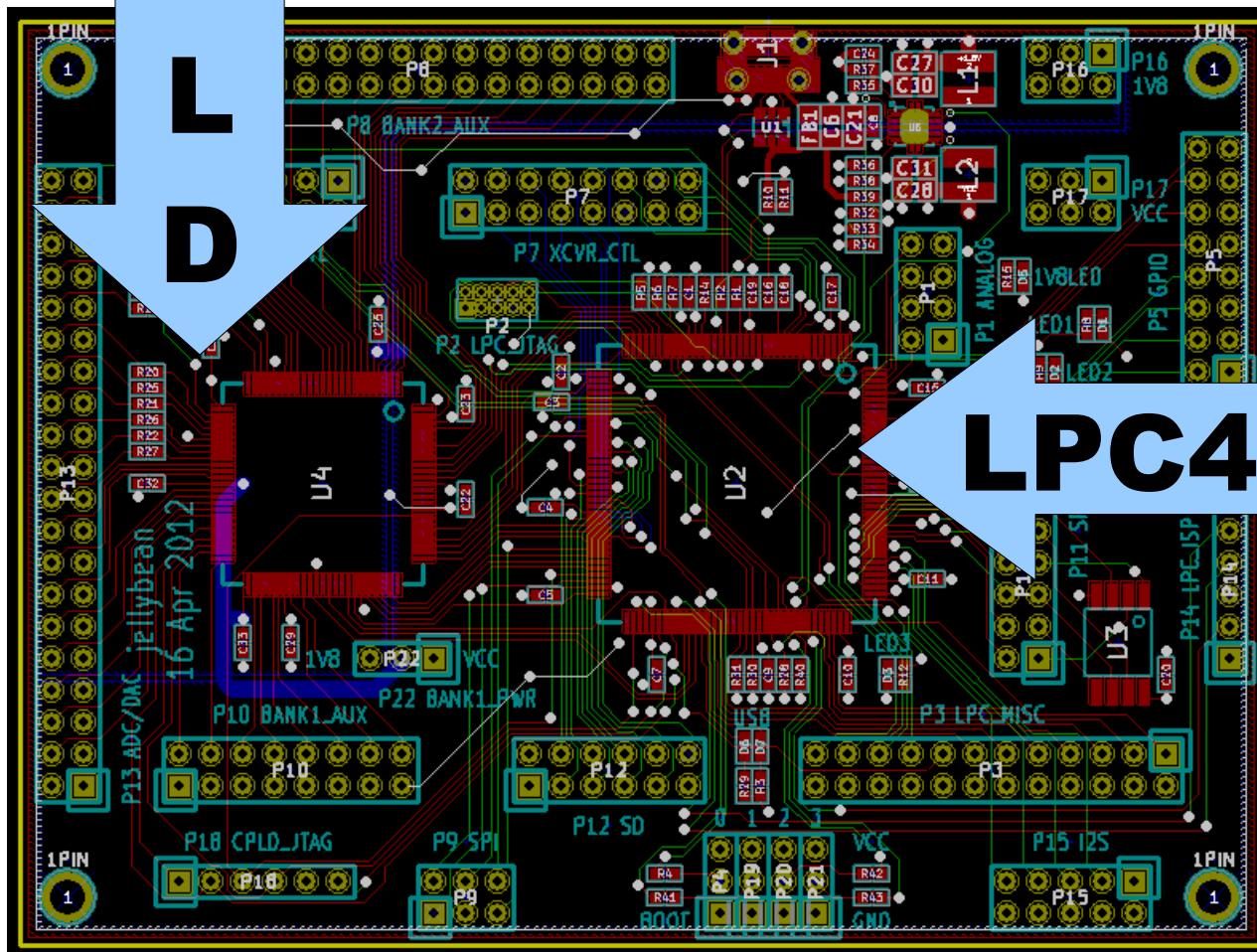
Designer **Consultant**

Retrospective HackRF HW

- **1st Board**
MCU/CPLD
Jellybean
16 Apr 2012



Restrospective Jellybean



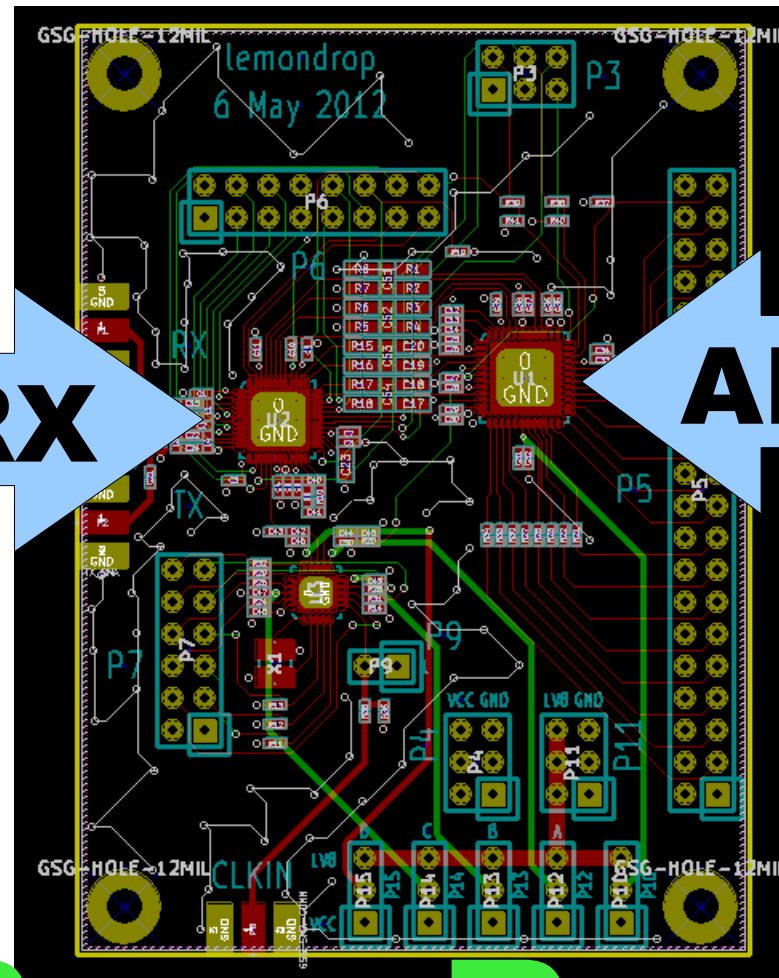
Digital

Retrospective HackRF HW

• **2nd Board**
Lemondrop
6 May 2012



Restrospective Lemondrop



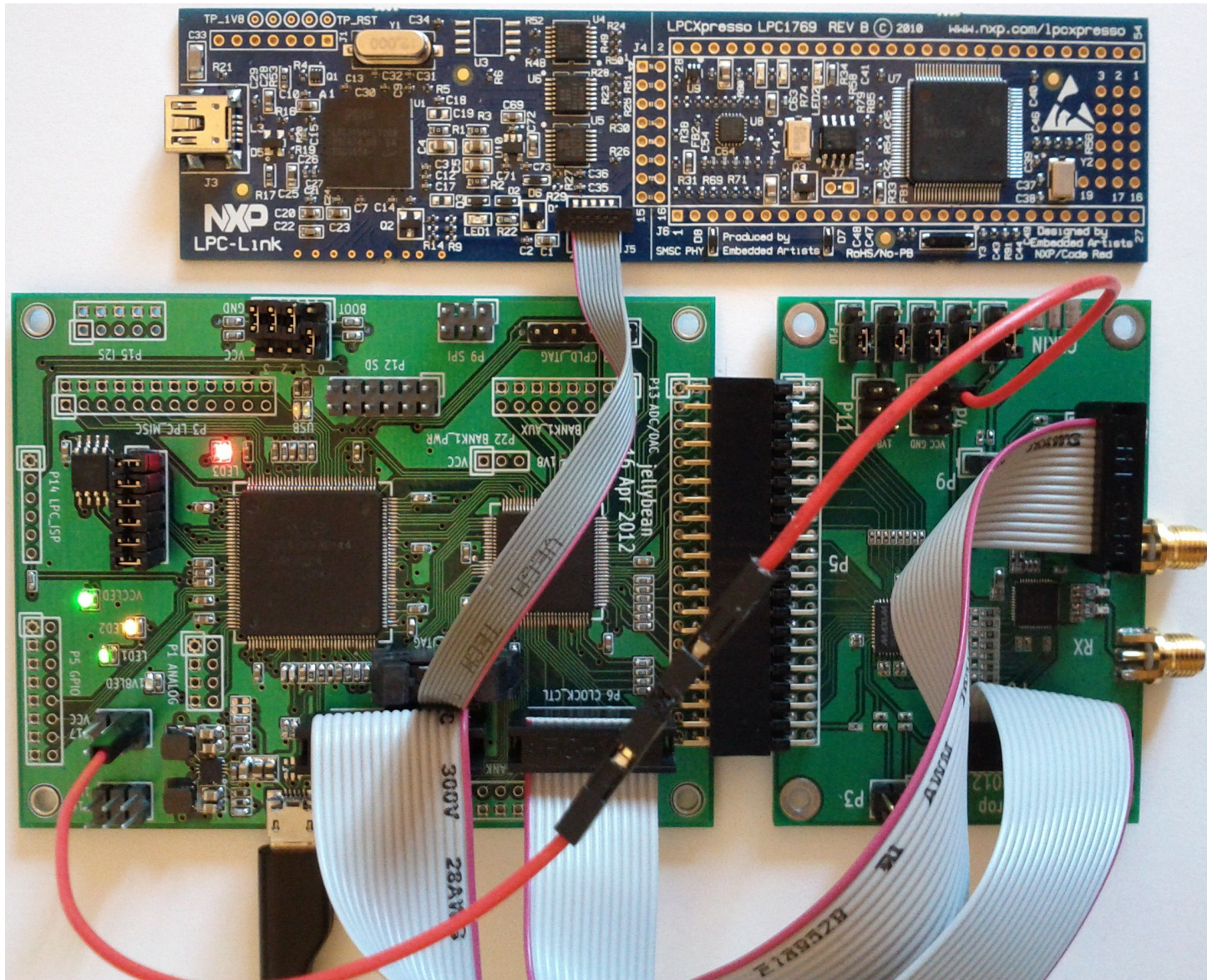
RF TX/RX

ADC/DAC

**2.3 -
2.7 GHz**

Base Band

JellyBean & LemonDrop



Retrospective HackRF HW

• **3rd Board**

Lollipop

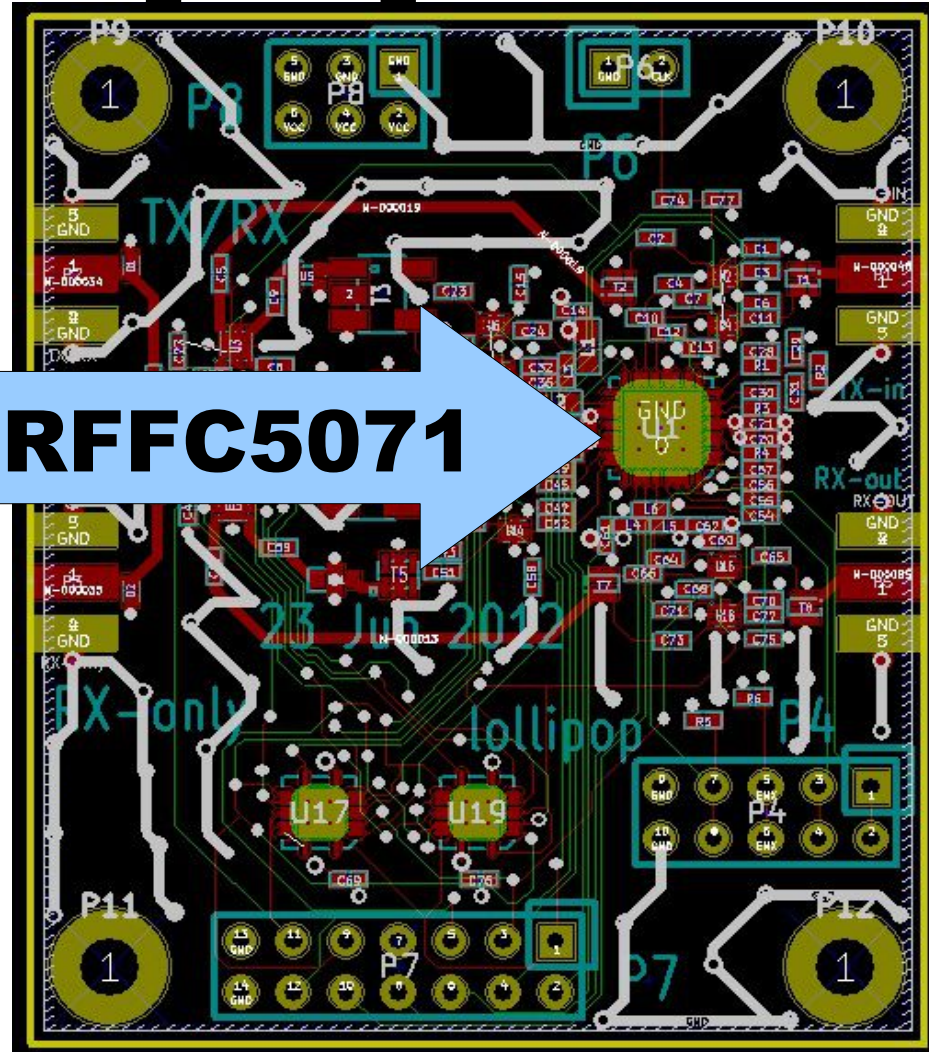
23 Jun 2012



Restrospective Lollipop

**SYNTHESIZER
WB
30MHz-6GHz
MIXER GHz**

RFFC5071



Front End

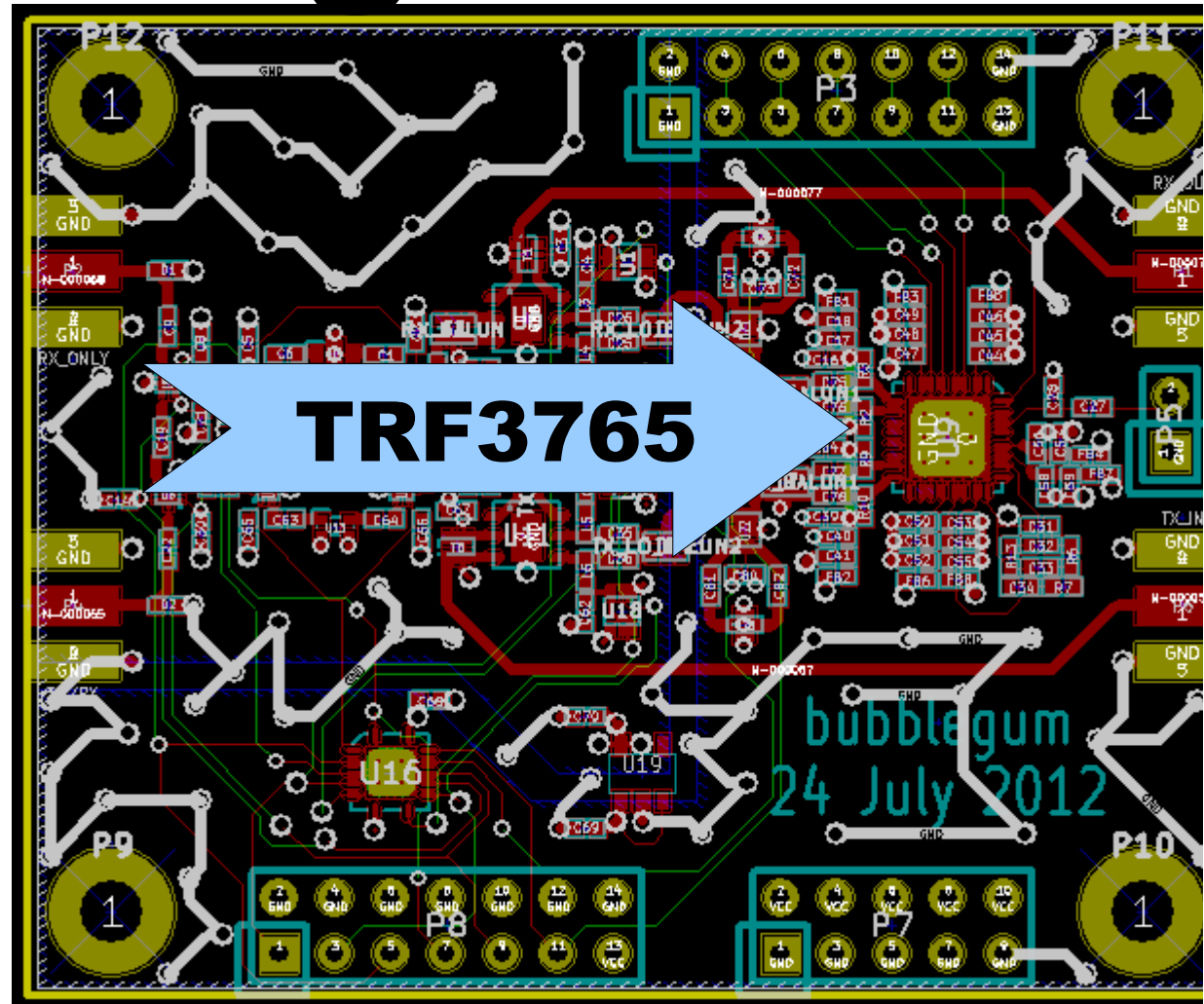
Retrospective HackRF HW

**•4th Board
Bubblegum
24 July 2012**



Restrospective Bubblegum

**SYNTHESIZER
WB
300MHz-4.8GHz
MIXER GHz**



Front End

Retrospective HackRF HW

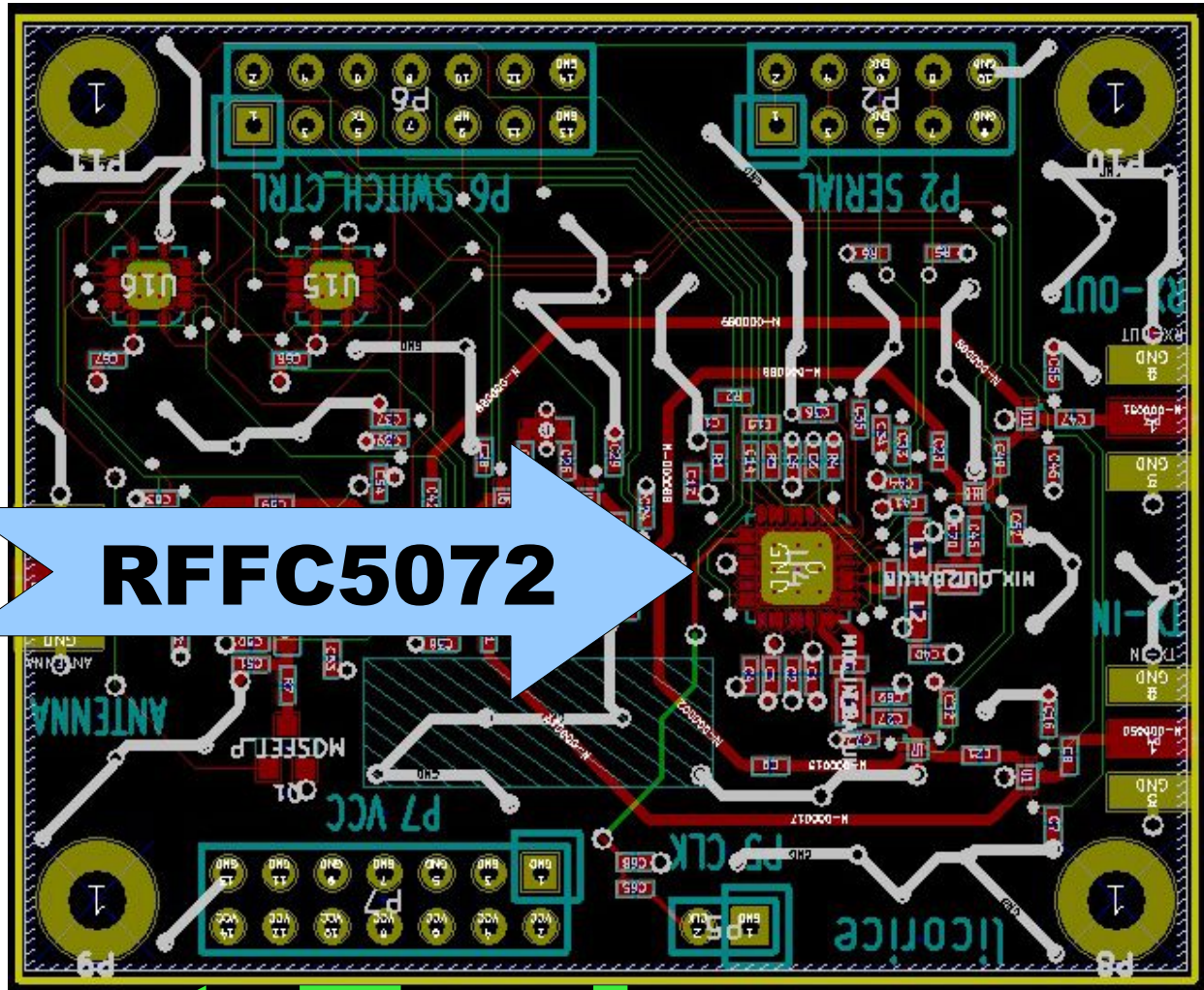
•5th Board

Licorice

27 Aug 2012



Restrospective Licorice



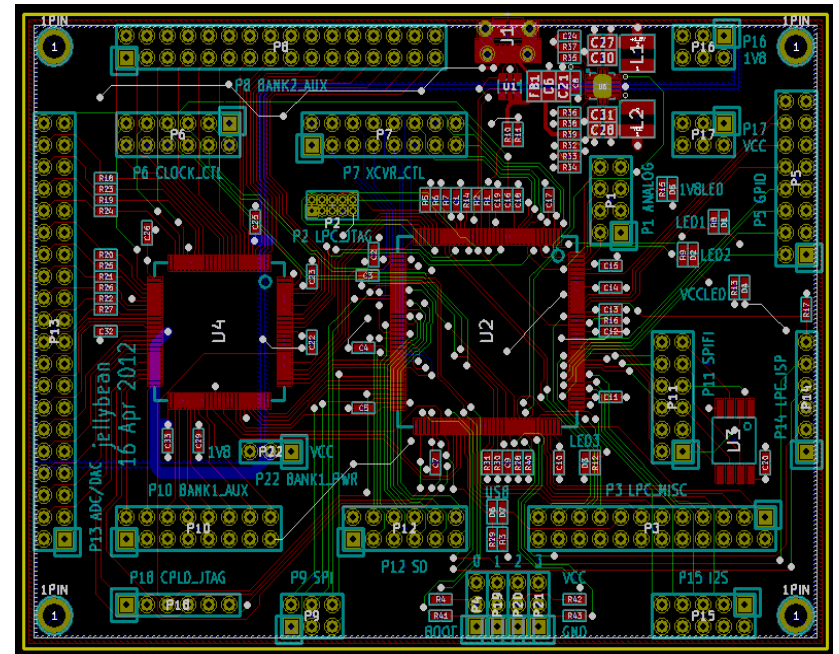
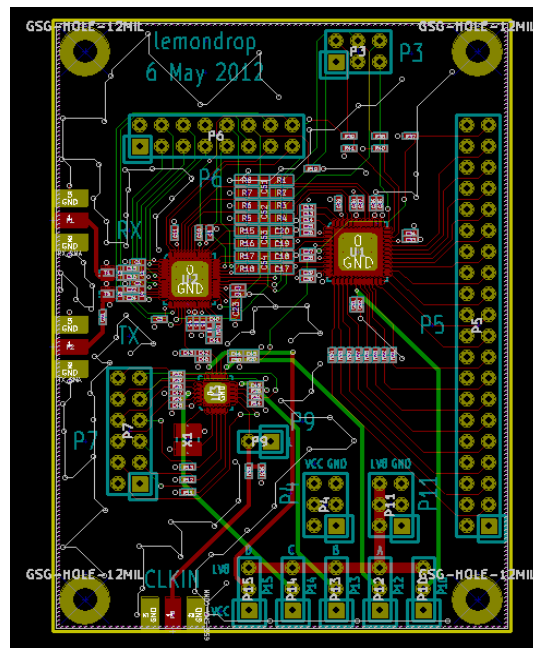
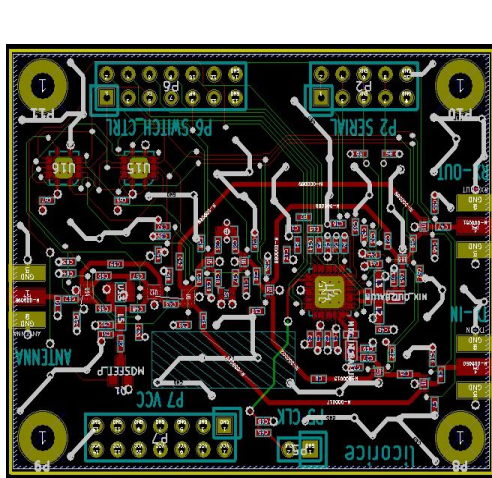
SYNTHESIZER
WB
30MHz-6GHz
MIXER GHz

RFFC5072

Front End

Restrospective

All in one



HackRF HW

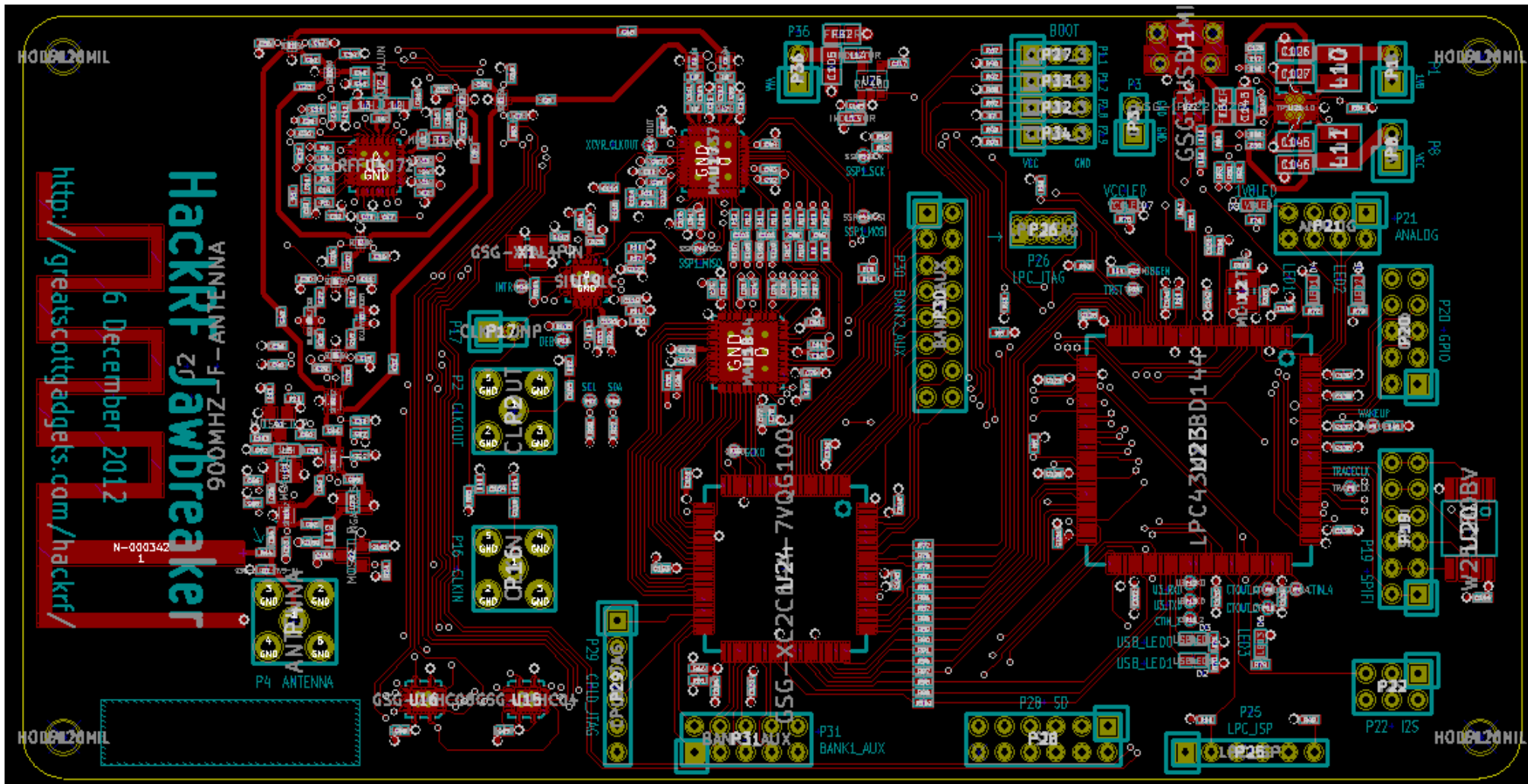
•6th Board

Jawbreaker

6 Dec 2012



HackRF Beta Board

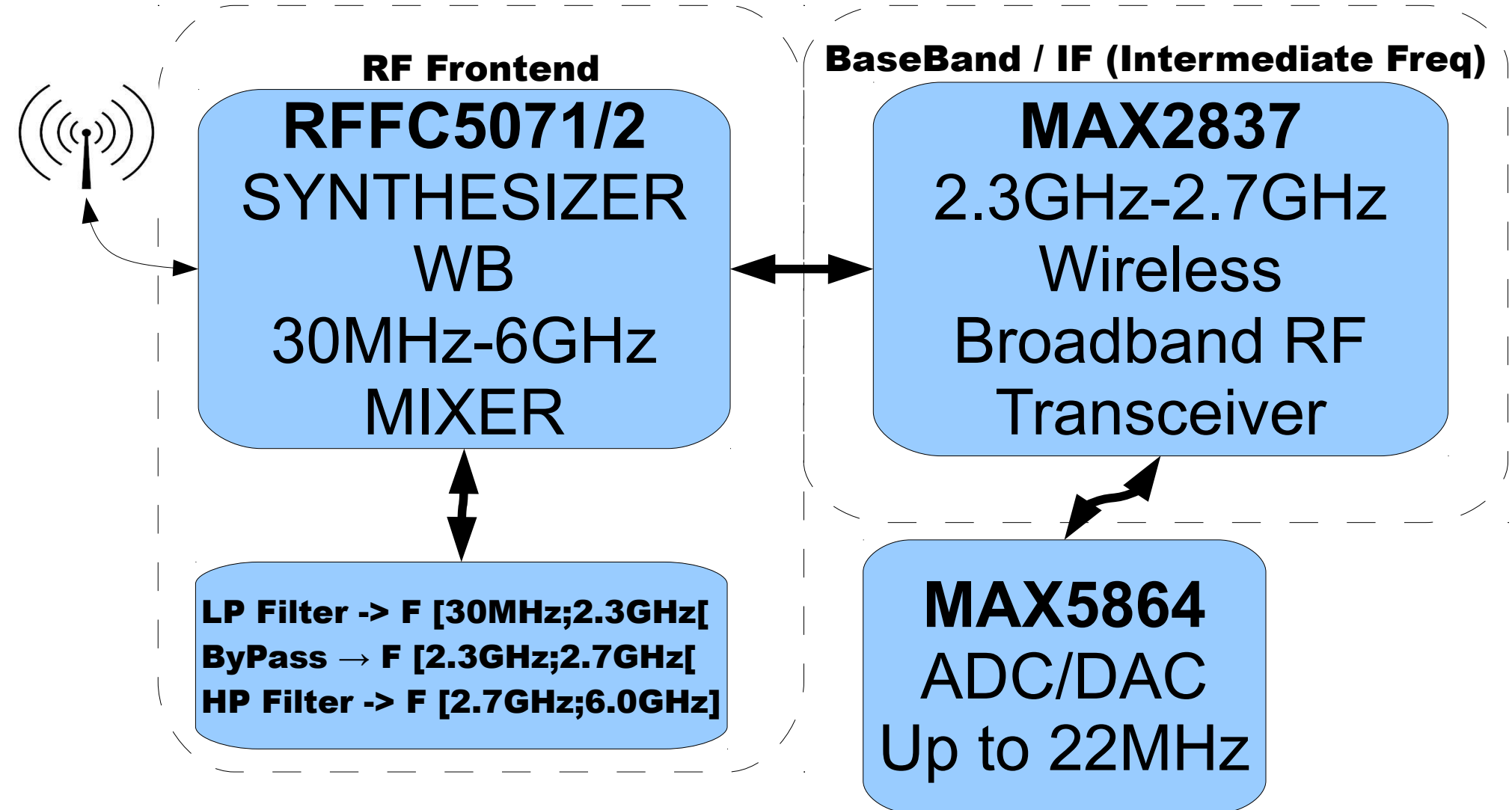


Jawbreaker

Jawbreaker HW

- **More than 300 components**
- **Majority of components are 0.4mm×0.2mm (0402 R&C)**
- **More than 25 IC**
- **About 2 days of manual assembly and testing for one board**

HackRF Frontend/BaseBand

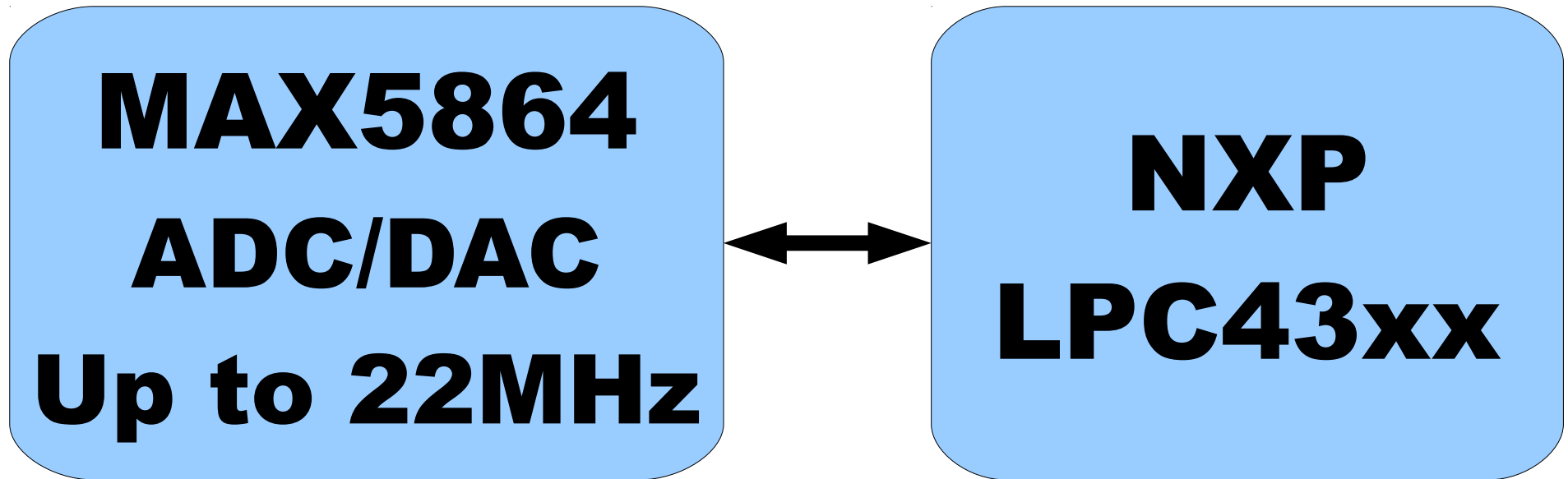


RF Frontend: Generic term for all the circuitry between the antenna and the first intermediate frequency (IF) stage
http://en.wikipedia.org/wiki/RF_front_end

Baseband refers to the original frequency range of a transmission signal before it is converted, or modulated, to a different frequency range

<http://www.techterms.com/definition/baseband>

HackRF Digital Stage



**Maximum 20MHz ADC/DAC
limited by USB2 HS
(about 40MiB/s)**

HackRF Clock

Flexible clock generation

Si5351

CLK0: MAX5864/CPLD

CLK1: CPLD ($2 * \text{CLK0}$)

CLK2: MCU SGPIO ($2 * \text{CLK0}$)

CLK4: 50MHz RFFC5071/2

CLK5: 40MHz MAX2837

HackRF Jawbreaker

HS USB 2.0
(40MiB/s)

BusPowered
(max 500mA)

30MHz to
6GHz OpFreq

Half-Duplex
Transceiver

20MHz Max
BW

Open Source
HW & SW

Defense Advanced Research Projects

**Agency
(DARPA)**

**Cyber Fast Track
(CFT)**

**This is a big
project for us.**

**This isn't a big
project for DOD.**

**The World
needs
Open Source
Hardware for
SDR**

Public Process

GitHub Explore GitHub Search Features Blog Sign up for free Sign in
github.com/mossmann/hackrf ★ Star 179 Fork 19

Code Network Pull Requests 0 Issues 0 Wiki Graphs

low cost software radio platform — [Read more](#)

[Clone in Windows](#) [ZIP](#) [HTTP](#) [SSH](#) [Git Read-Only](#) [Read-Only access](#)

branch: **master** Files Commits Branches 2 Tags 3

hackrf / [+](#)

[825 commits](#)

Merge pull request #45 from TitanMKD/master ...

mossmann authored 21 days ago latest commit 99c8055d15

doc	24 days ago	HackRF Jawbreaker Boot Mode [TitanMKD]
firmware	21 days ago	Cleanup on xxx_rom_to_ram directory now it contains only makefile, re... [TitanMKD]
hardware	24 days ago	Merge pull request #43 from TitanMKD/master [mossmann]
host	21 days ago	hackrf_spiflash modified -l argument is not used anymore with -w argu... [TitanMKD]
test_max2837	11 months ago	Tests for MAX2837 with OLS Capture. [TitanMKD]
COPYING	a year ago	readme and license files [mossmann]
Readme.md	7 months ago	readme fix [mossmann]
TRADEMARK	a year ago	readme and license files [mossmann]

Public Process

github.com/mossmann/libopencm3

Code Network Pull Requests 0 Wiki Graphs

Clone in Windows ZIP HTTP SSH Git Read-Only <https://github.com/mossmann/libopencm3.git> Read-Only access

branch: master Files Commits Branches 1 Tags

libopencm3 / 821 commits

Merge pull request #20 from TitanMKD/master

mossmann	authored a month ago	latest commit 701c23ada9
examples	4 months ago	lpc43xx basic IPC for multicore M4 & M0 (with basic examples for hack... [TitanMKD])
include	4 months ago	lpc43xx basic IPC for multicore M4 & M0 (with basic examples for hack... [TitanMKD])
lib	a month ago	Cleanup M0 makefile to avoid copying file from lpc43xx(M4) directory. [TitanMKD]
scripts	7 months ago	Change header generation script to produce function-like #define macr... [jboone]
.gitignore	a year ago	Filled in the APB0 memory map for the 17... [dreddor]
COPYING.LGPL3	a year ago	License change of the library to LGPL, version 3 or later. [esden]
Doxyfile	a year ago	Doxyfile: Configure for libopencm3 needs. [uwehermann]
Makefile	4 months ago	lpc43xx basic IPC for multicore M4 & M0 (with basic examples for hack... [TitanMKD])
README	a year ago	License change of the library to LGPL, version 3 or later. [esden]

See us also on IRC

Freenode channel #hackrf

Volunteers !

**Everyone is
welcome to help
us developping
SDR tools**

TOOLS

Kicad

GCC

Gnu Radio

SDR#

100%

NDA

Free !

NXP LPC43xx

ARM Cortex

DualCore

M4F + M0 @ 204 MHz

SGPIO + FPU(32bits)

HS USB 2.0

libopencm3

Thank you !

DARPA CFT

BIT Systems

Michael Ossmann

Jared Boone

Youssef

Hackito

Touil

HackRF links

<http://greatscottgadgets.com/hackrf>

HackRF beta

<https://greatscottgadgets.com/forums/hackrf-beta-reg.html>

And Now

DEMO !!

HackRF Host Tools

Windows/Linux

- **hackrf_info (board info/ident)**
- **hackrf_cpldntag (update CPLD)**
- **hackrf_max2837 / rffc5071 / si5351c (R/W registers)**
- **hackrf_spiflash (update fw)**
- **hackrf_transfer (RX/TX)**

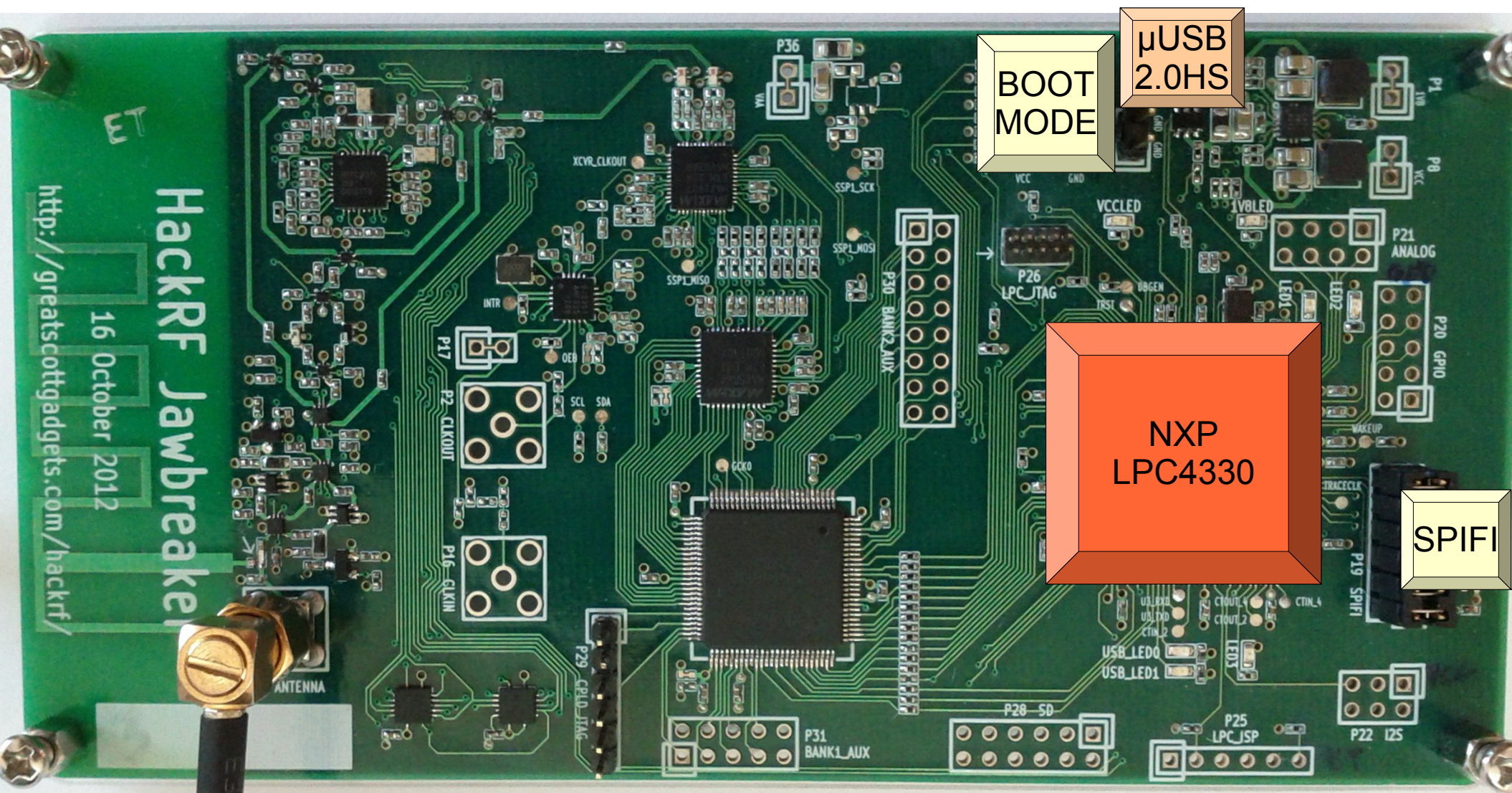
HackRF SDR# FM DEMO

HackRF SDR# Talkies DEMO

HackRF SDR#

DECT Phone DEMO

BONUS



NXP LPC4330

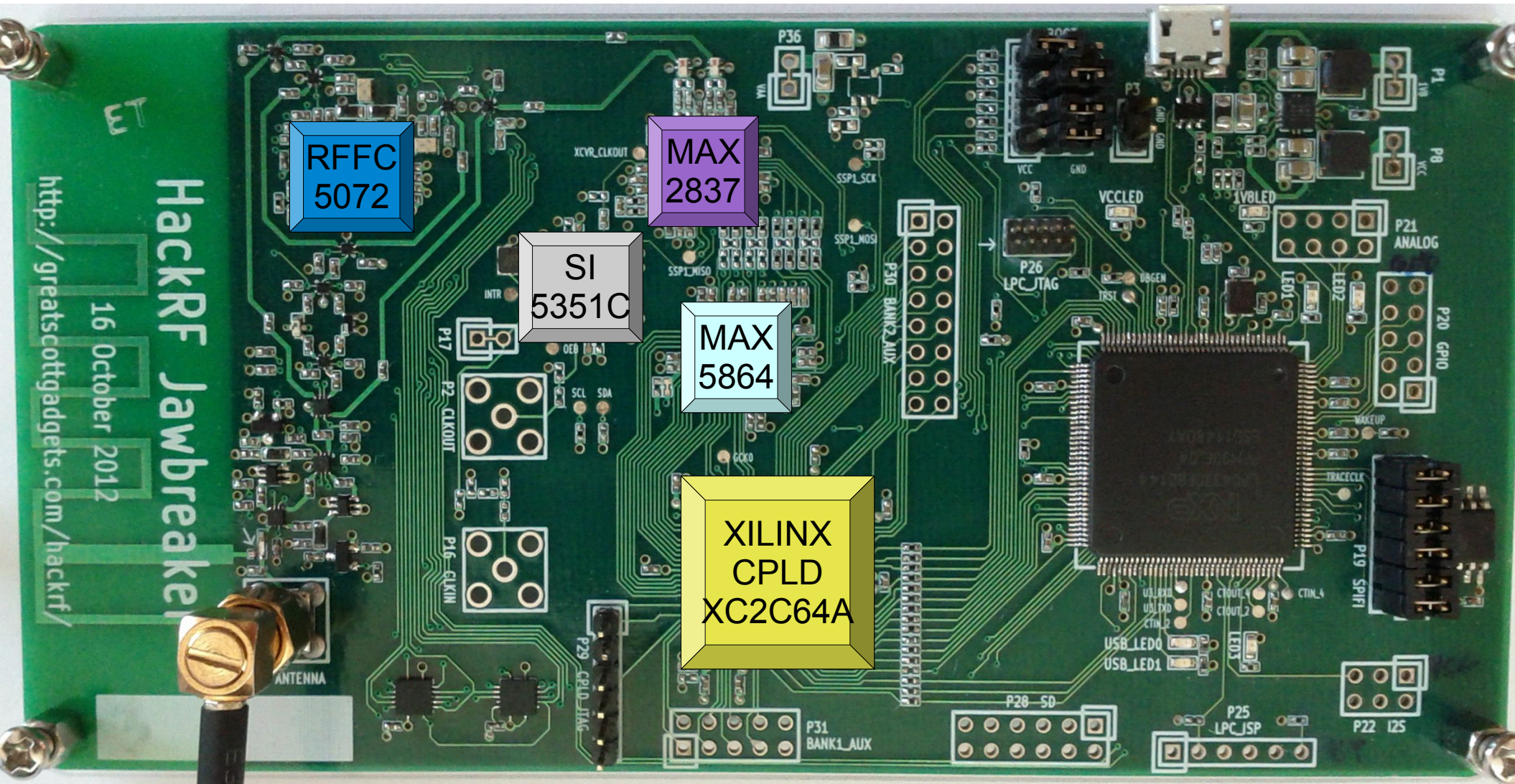
- Dual Core MCU M4+FPU & M0
- 204 MHz, 264KB SRAM
- High Speed USB 2.0
- SGPIO (used for ADC/DAC up to 40MHz IQ with 20MHz ADC/DAC)
- Open Source development using libopencm3 (LGPL v3)

BOOT MODE

- SPIFI Boot
- USB0 (Recovery mode)

SPIFI

- 1MB SPIFI boot
- Code => SRAM



RFFC5072

- Wideband synthesizer/vco withintegrated 6GHz mixer

SI5351C

- Clock generator and VCXO
- Up to 8 independant Clocks

MAX 5864

- ADC / DAC up to 22MHz
- 8 bits ADC and 10bits DAC

MAX 2837

- 2.3GHz to 2.7GHz Wireless Broadband RF Transceiver

XILINX CPLD

- Mainly used for synchro with SGPIO & MAX5864