RTL Entropy

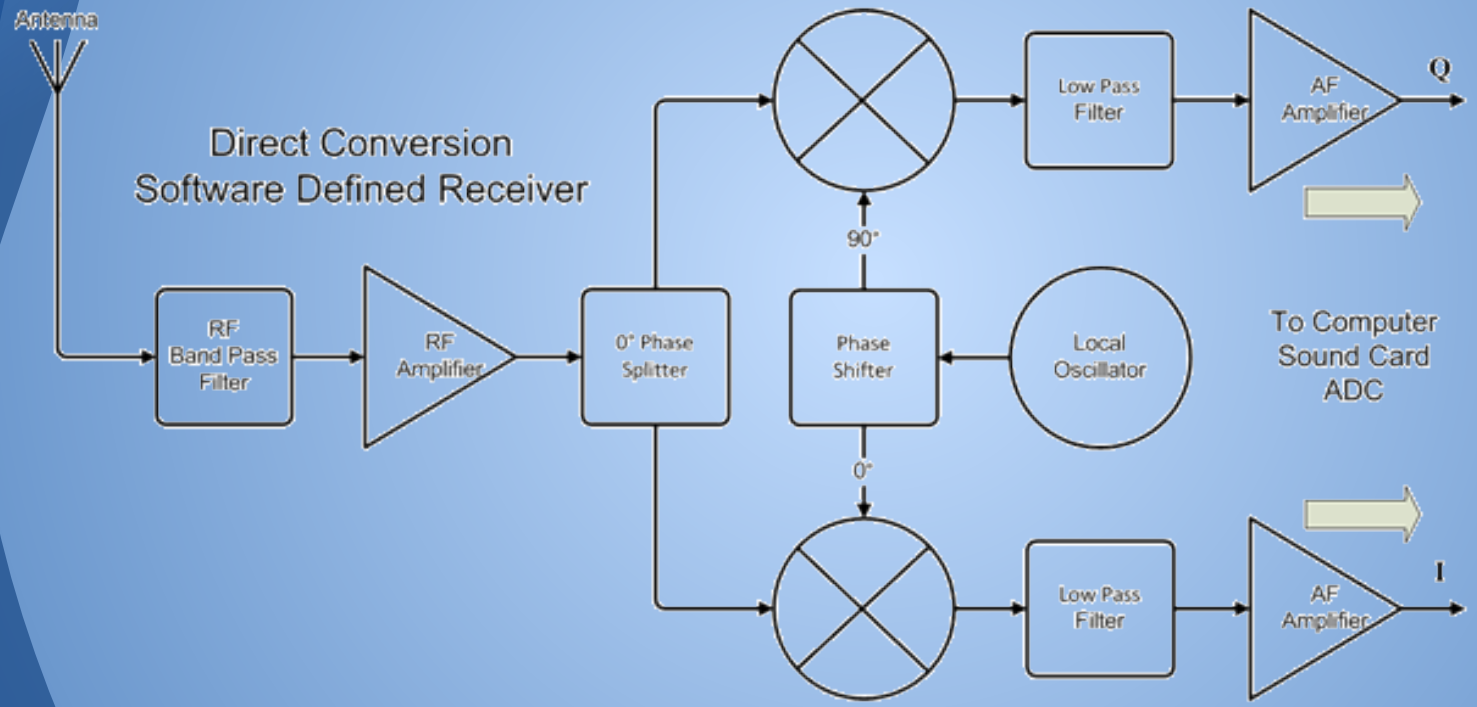
$30 3Mb/s entropy source

Software Defined Radio

Electronics:
Antenna ->
Lots of complex thingies ->
Output

Antenna ->
Quadrature Sampling Detector ->
ADC ->
Software ->
Output

Quadrature Sampling Detector



Maths = Electronics

$$\left[0.9\left[\frac{A+B}{2}+\frac{A-B}{2}\sin 4\pi f_p t\right]+0.1\sin 2\pi f_p t\right]\times 75\ \text{kHz}$$

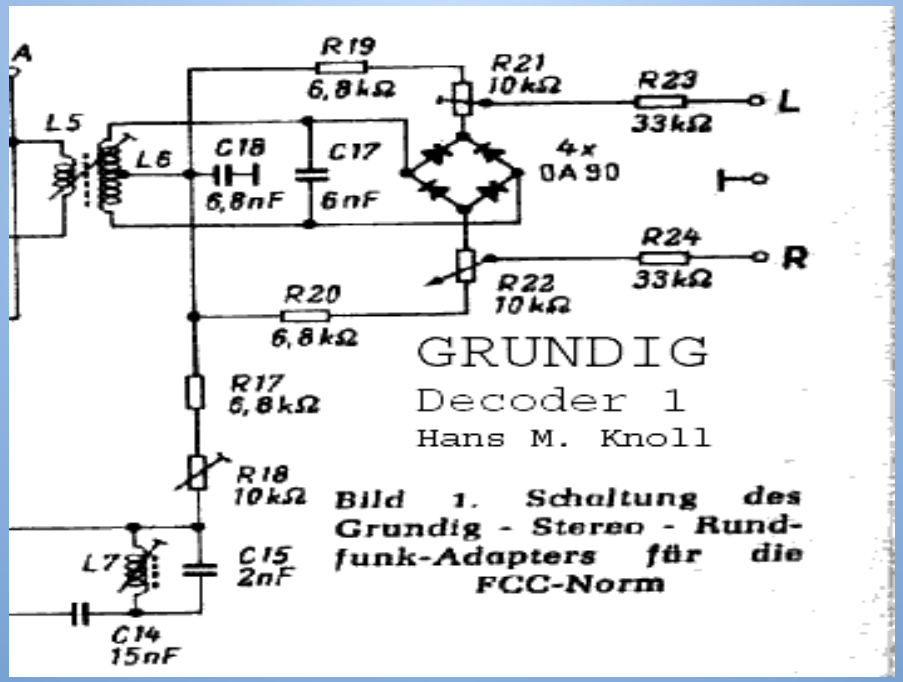


Bild 1. Schaltung des Grundig - Stereo - Rundfunk-Adapters für die FCC-Norm

= Code

```
for (var i = 0; i < length; i++) {
                var pilot = _pilotFilter->Process(baseBand[i]);
                _pll->Process(pilot);
                _channelBPtr[i] = baseBand[i] * Trig.Sin((float) (_pll->AdjustedPhase * 2.0));
        }
for (var i = 0; i < audioLength; i++)
        {
                var a = _channelAPtr[i];
                var b = 2f * _channelBPtr[i];
                interleavedStereo[i * 2]     = (a + b) * AudioGain;
                interleavedStereo[i * 2 + 1] = (a - b) * AudioGain;
        }
```

RTL-SDR

- Cheap USB DVB-T/DAB+/FM
- DAB+ and FM done in software

Antti Polassari discovered this.
Osmocom-SDR wrote the rtl-sdr C libraries.
Others wrote GnuRadio blocks, other apps

GQRX Demo.

Informational Entropy

Lots of maths see https://en.wikipedia.org/wiki/Informational_entropy

Boils down to: a data sequence has high entropy when you can't beat 50/50 odds on predicting the next bit given all previous bits.

Entropy Sources

- Classical
  - Atmospheric Radio
  - Amplifier Noise
  - Coupled Oscillators
  - Reverse Bias Diodes
- Quantum
  - Quantum Vacuum Noise (On campus, 2Gb/s)
  - Schottky Noise (photodiode excitation)
  - degenerate optical parametric oscillator

RTL-Entropy

- Reads 6 LSB of 8 bit I/Q samples
- Does Von Neumann debiasing
- Sends to FIPS 140-2 test library
- XOR with previous buffer if passed
- Output!

Works well, at about 5Mb/s
Daemon mode included for interaction with rngd to add entropy to the kernel

Cryptography Concerns

- Atmospheric Radio inherently insecure!
  - Wideband FM doesn't have much effect
  - we still get entropy from the amplifier noise and ADC aliasing.
- Short the antenna with a 50Ω load
- put in shielded box
- Amplifier Noise, harder to mess with

More Debiasing Needed?

This is where I start getting hazy

Kaminsky Debiasing, Does it help?

- SHA512(discarded bits from Von Neumann step)
- Encrypt entropy with hash
- I think…

Is XORing on old entropy good/bad?

Just following what some dude on the internet said!

Thanks!

https://github.com/pwarren/rtl-entropy