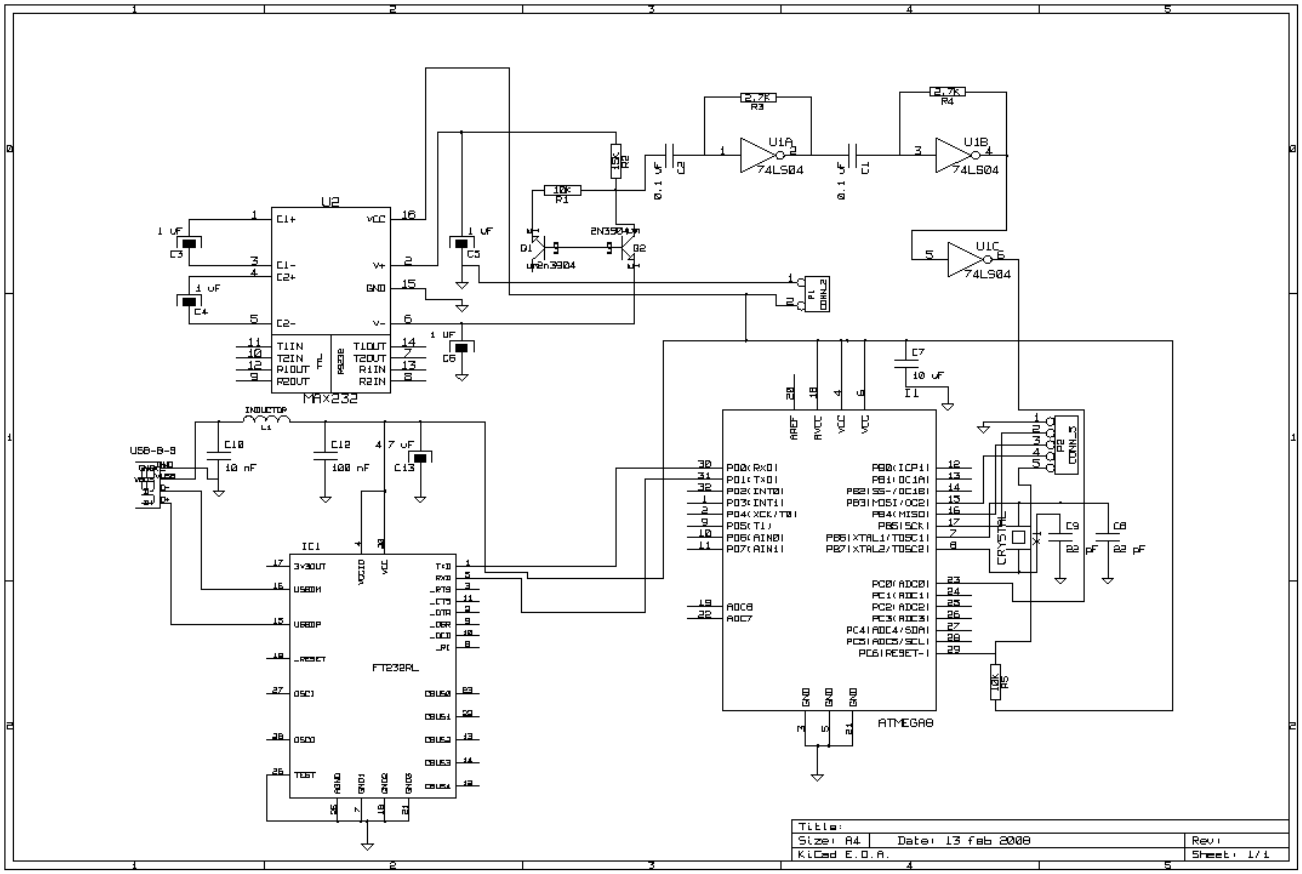
Hardware RNG kit:

Schematic:



Parts List:

Capacitors:

C1 0.1 uF
C10 10 nF
C12 100 nF
C13 4.7 uF
C2 0.1 uF
C3 1 uF
C4 1 uF
C5 1 uF
C6 1 UF
C7 10 uF (or substitute 4.7uF or 1uF)
C8 22 pF
C9 22 pF

Semi/IC:

I1 ATMEGA8
IC1 FT232RL
Q1 2n3904
Q2 2N3904
U1 74LS04
U2 MAX232

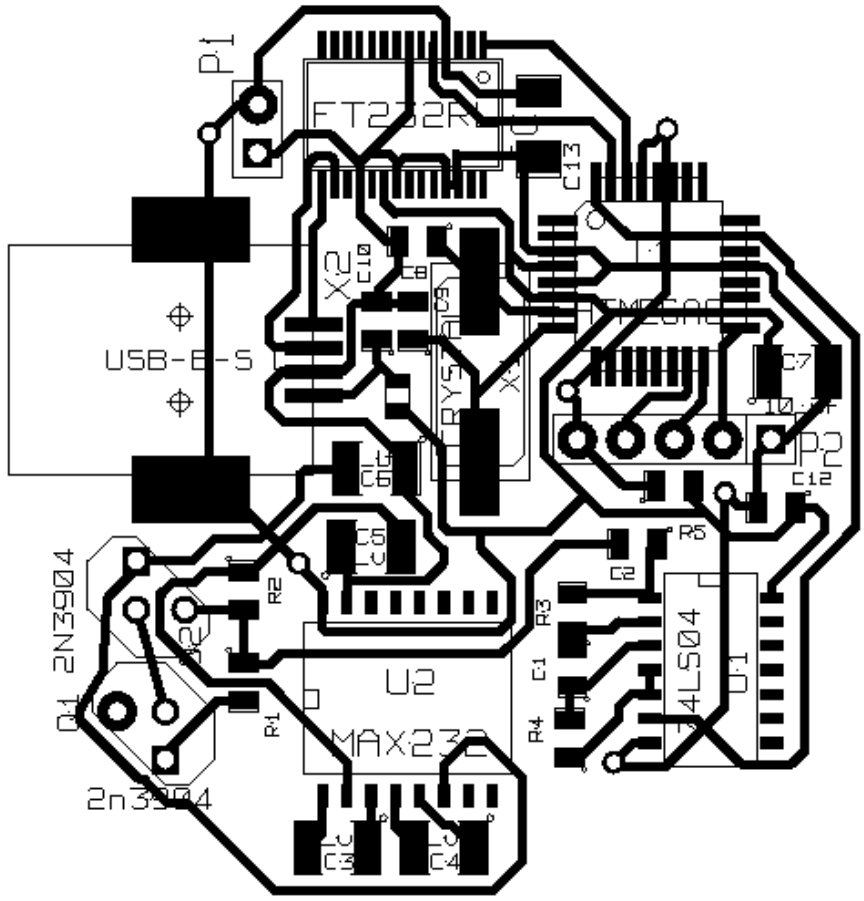
Misc:

L1 INDUCTOR
X1 CRYSTAL
X2 USB-B-S
P1 CONN_2 (power connector for external)
P2 CONN_5 (programming header)

Resistors:

R1 10K
R2 15K
R3 2.7K
R4 2.7K
R5 10K

Placement:



Description:

"This circuit uses avalanche noise in a reverse-biased PN junction, the emitter-base junction of the first transistor. The second transistor amplifies it. The first two ALS04 inverters are biased into a linear region where they act like op amps, and they amplify it further. The third inverter amplifies it some more..."

[Will Ware]

The RS232 IC is used to generate a 20V potential for the transistor. The white noise spectrum should be flat with no one frequency dominating. This white noise signal is squared up by the inverter and sampled by the ATmega8 on a single digital input pin. Tthe signal is also routed to pin 32 (INT0) for alternative code functionality. A simple programming header allows for HEX upload of sampling and serial code. The board is attached by way of USB serial interface and outputs a stream of random bytes.

Construction notes:

Follow placement diagram with USB connection to the left as above. Start by soldering all SMD/surface mount components first. Finally solder jumper wires, programming header and USB connector. Pay attention to polarity of capacitors (electrolytic), and orientation of ICs (see dots or indents marking), and the two 2n3904 transistors (these are the reverse of indicated above - the backs are facing the other way). Once the board is assembled it must be programmed and fuse bits set as follows:

avrdude -c avrisp2 -p m8 -P /dev/ttyUSB0 -U flash:w:code.hex

fuses:

avrdude -p m8 -u -c avrisp2 -t -v -v

w lf 0 0xff

w hf 0 0xdf

References:

http://1010.co.uk/tech_notes2.html

http://www.hcrs.at/

http://www.cryogenius.com/hardware/rng/

http://www.ciphersbyritter.com/RES/NOISE.HTM

http://robseward.com/itp/adv_tech/random_generator/

http://noosphere.princeton.edu/

http://www.baudline.com/