Affordable hardware random number generators (HRNGs)

Kenji Rikitake

りきたけ けんじ

力武 健次

27-NOV-2015
IPSJ IOTS2015 WIP
Chiba, Japan
@jj1bdx

Why HRNG?
Mandatory for security!

- **Keys: TLS, SSH, DNSSEC, passwords**
- ***Random number generators are the foundation for generating encryption keys***
- **Load balancing with minimal bias**
- **Fairness for gambling applications**

Why *original* HRNG?

- Required for *sufficient strength* of seeding /dev/[u]random
- Fast and more unpredictable seeding
- Fast enough to feed all applications through making /dev/[u]random sufficiently random

"OK then show us what you've got"

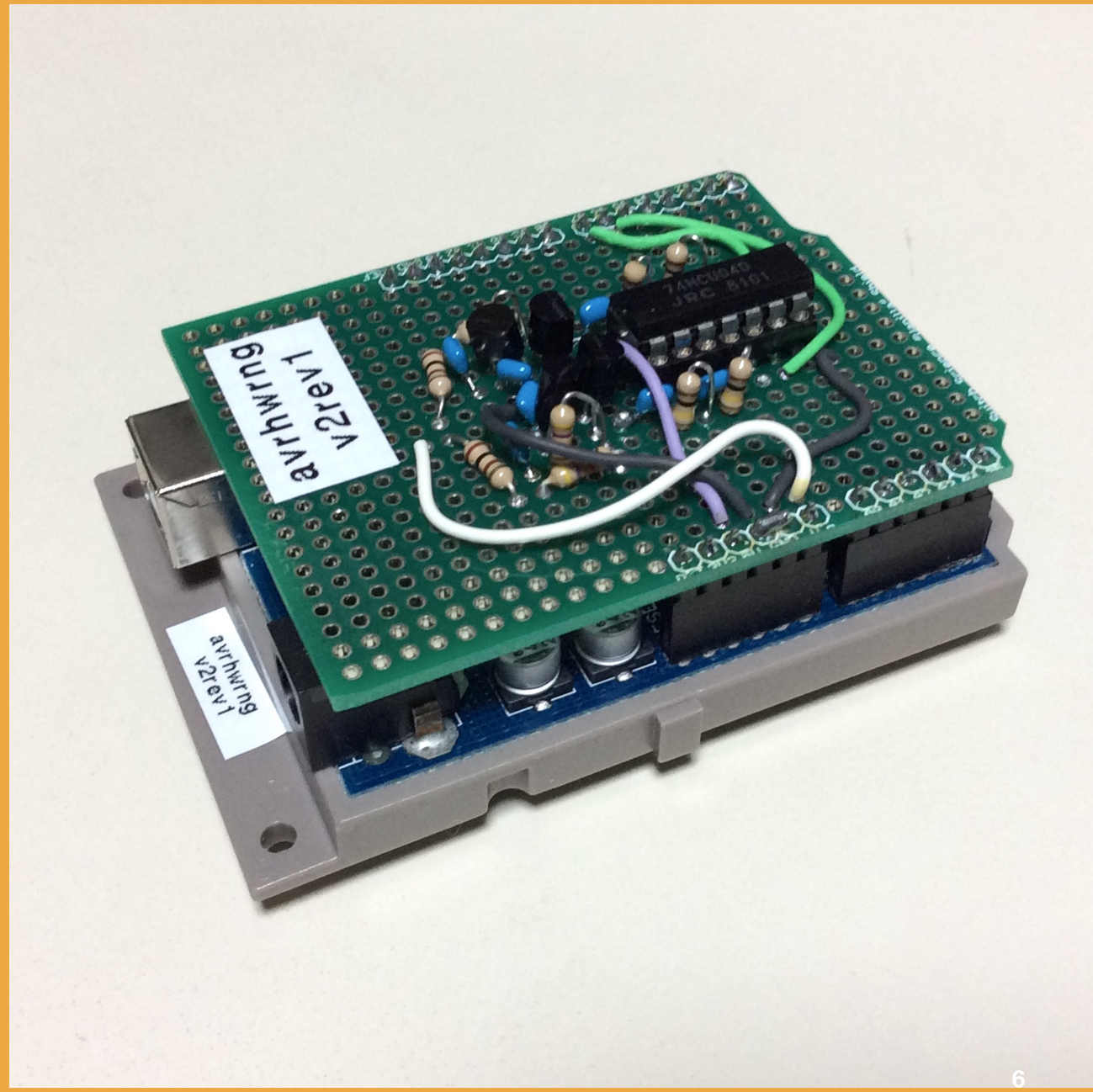
— avrhwrng
— ST Dongle for NeuG

Both are USB CDC-ACM devices

— Accessible as modem/tty devices

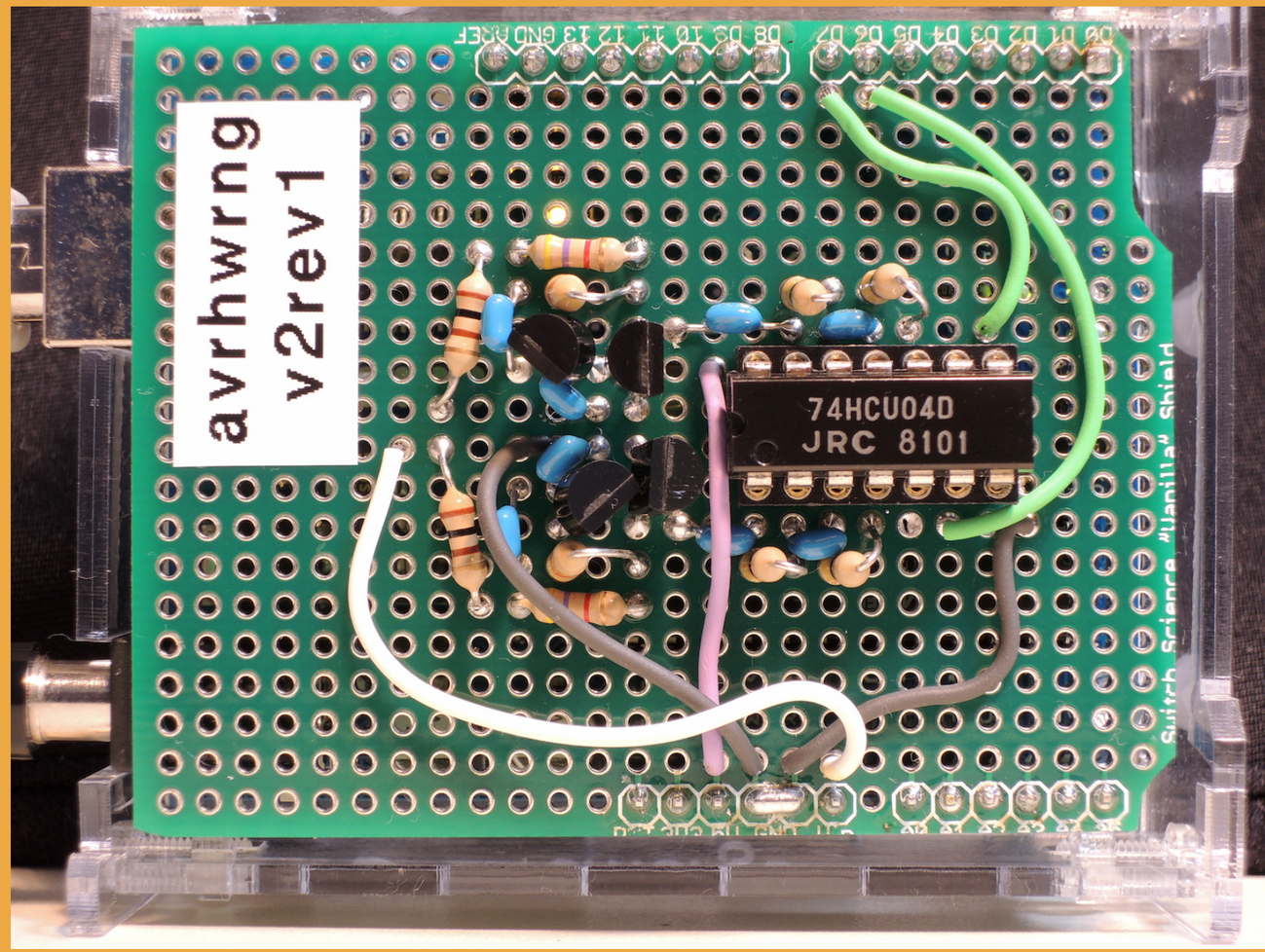
avrhwrng

- With 8bit AVR Arduino
- Reverse biased diodes
- ~10kbytes/sec (raw output: ~80kbytes/sec)
- DC 12V required
- Arduino shield



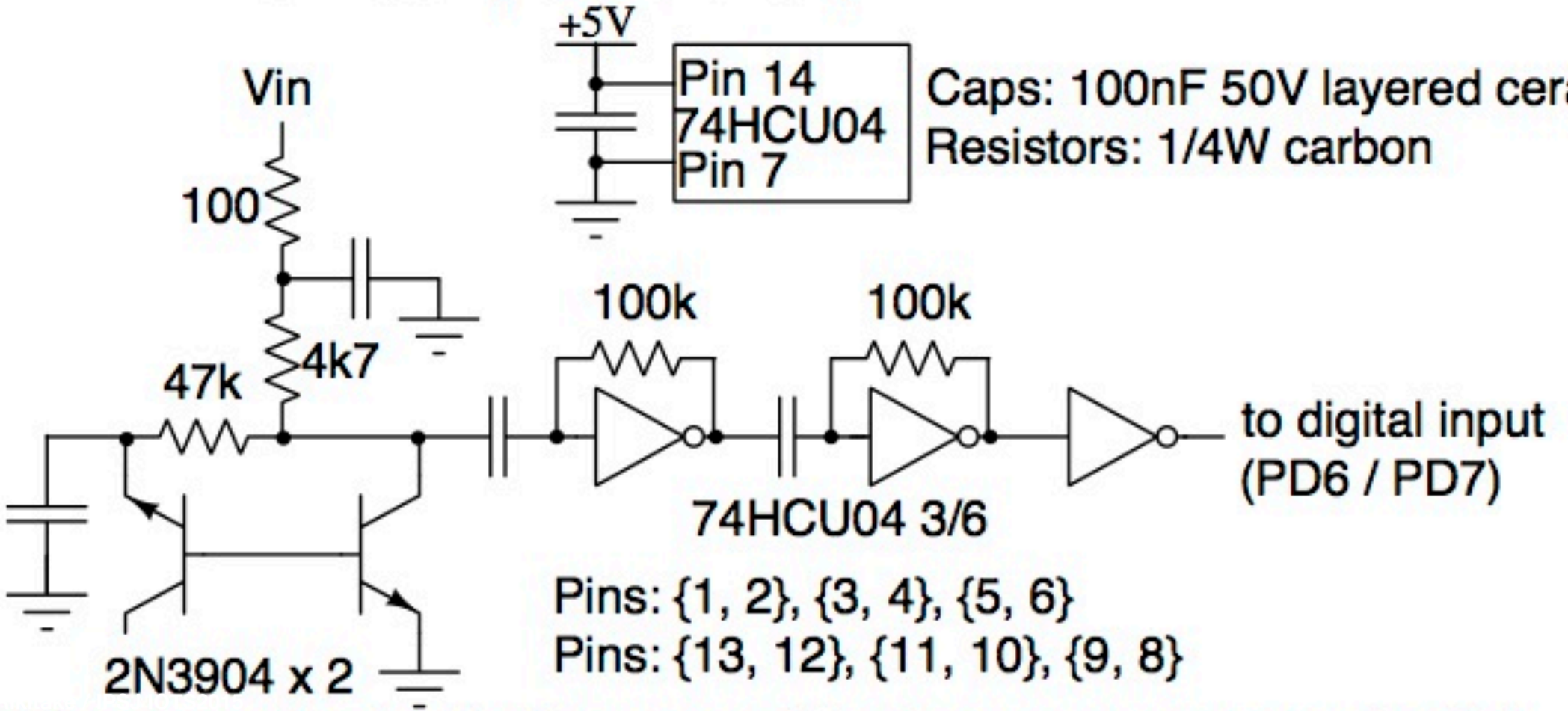
avrhwrng parts

- 74HCU04 x 1
- 2N3904 x 4
- All available in Akizuki Denshi
  秋月電子通商
- Parts cost: ~JPY500



avrhwrng: Arduino 2009/UNO shield schematics
for a hardware random number generator
by Kenji Rikitake / v2rev1 / 25-SEP-2015

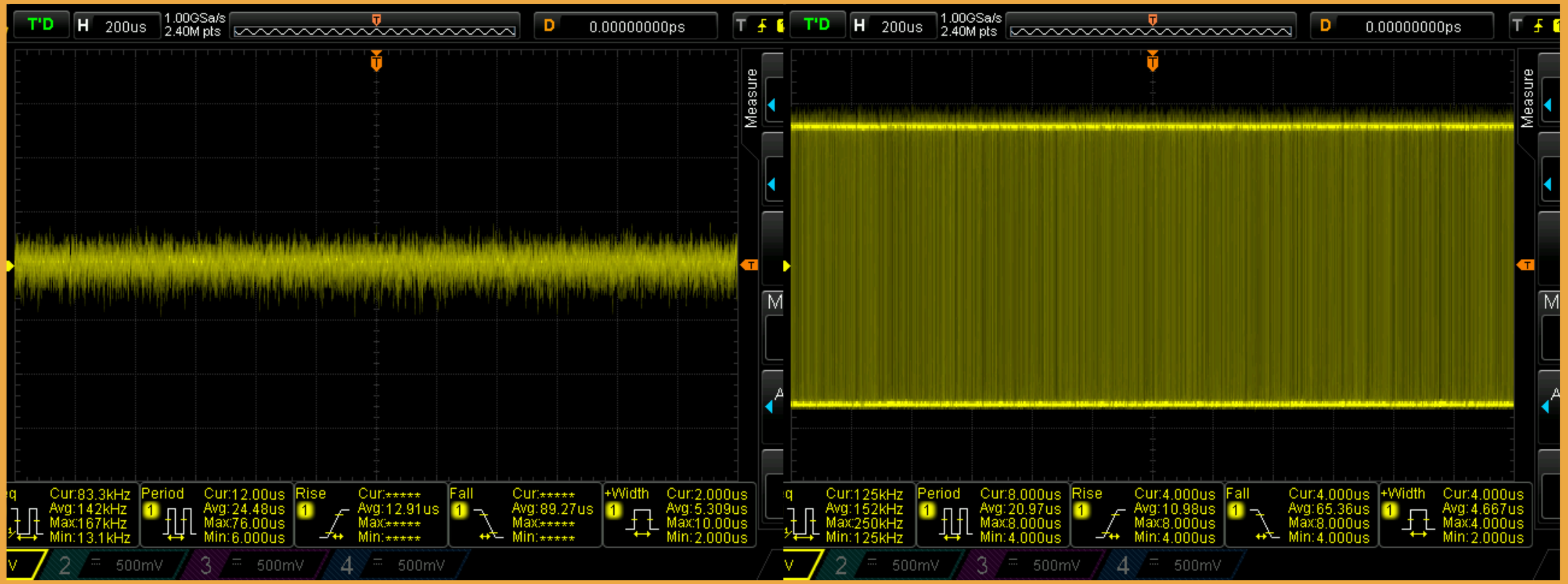
Vin = +12V or +13.8V (+9V didn't work)



Caps: 100nF 50V layered ceramic
Resistors: 1/4W carbon

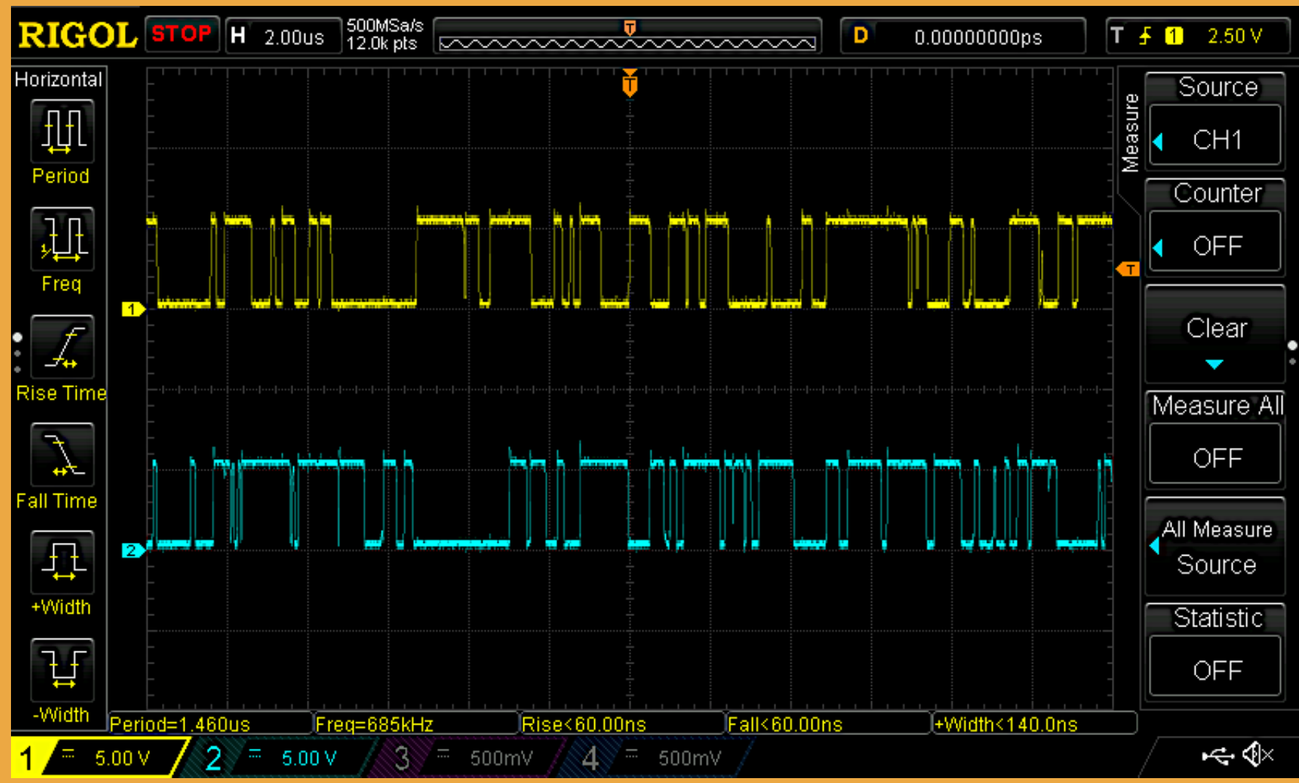
(The above circuit only shows one of the two same necessary circuits)

avrhwrng amplifiers



Why *two* diodes?

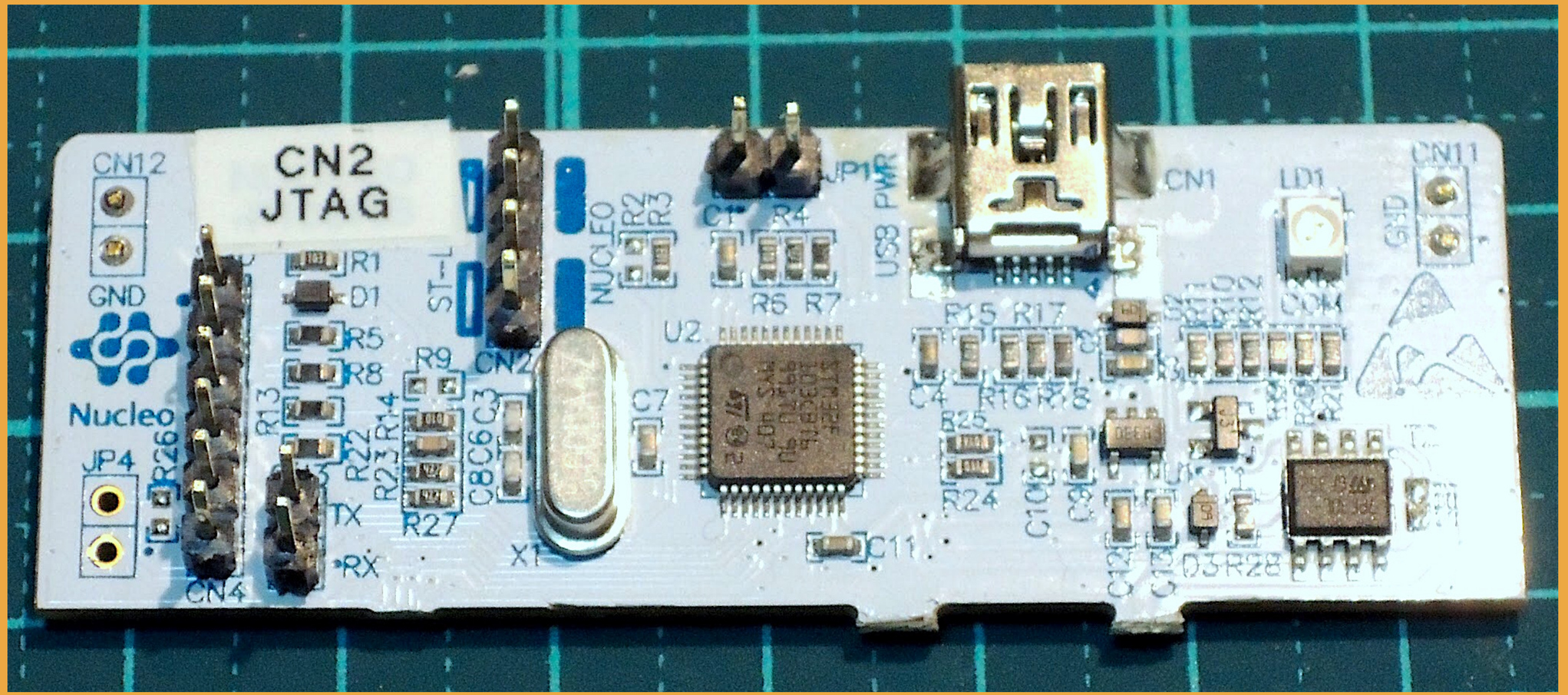
- Differential input for removing environmental common-mode effects
- ... Or simply two-bit parallelism
- Can be extended to more bits/ sample



NeuG

- Yutaka Niibe's GPLv3 HRNG software for ARM Cortex-M3 including Flying Stone's FST-01
- RNG for GnuK, a secure cryptographic token hardware usable on GnuPG and OpenSSH
- No external power required
- Using internal A/D converter noise as the randomness source
- ~80kbytes/sec (with internal whitening)

ST Dongle for NeuG



FreeBSD HRNG code

- Requires a device driver to use random_harvest(9) and rndtest(4)
- ... so I wrote a driver and feeder for FreeBSD 10.2-STABLE
- Working stably for months

On choosing hardware

Japanese semiconductors are no longer available **for prototyping: use (American) well-known semiconductors instead (e.g., 2SC1815 -> 2N3904)**

For more applications

- Stable operation infrastructure needed for fault tolerance
- Expertise on production-level cases (e.g., DNSSEC, PKI key generation)
- We need more internal information for seeding the system PRNG by the external devices: Windows? OS X? Android? iOS? Other proprietary platforms?

My codes and docs in GitHub

https://github.com/jj1bdx/avrhwrng

Thanks

Questions?