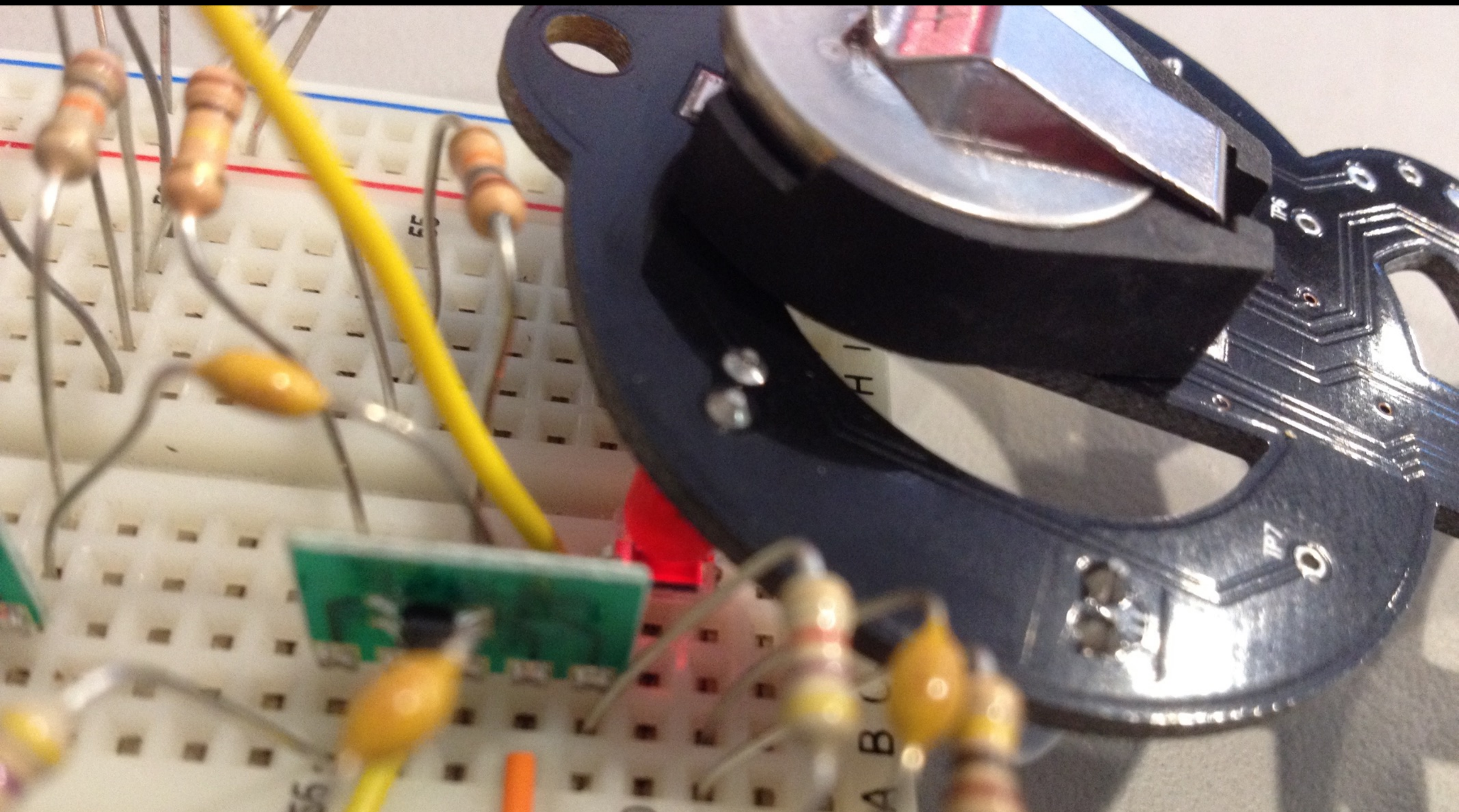
OPTICAL COVERT CHANNELS

Joe Grand (@joegrand)



Covert Channels

- Hidden methods to exfiltrate/transfer data from an apparent normally functioning system
- Could be achieved with HW and/or FW modification
  - Specifications modified or misdesigned before manufacturing
  - On physical device during manufacturing or in-the-field
  - Hardware implant via interdiction

Exploiting the Environment

- Leakage based on optical, acoustic, thermal, or RF characteristics of a system
  - Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations (Kuhn, Anderson)
  - Inaudible Sound as a Covert Channel in Mobile Devices (Deshotels)
  - BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations (Guri, Monitz, Mirski, Elovici)
  - Emanate Like a Boss: Generalized Covert Data Exfiltration with Funtenna (Cui)

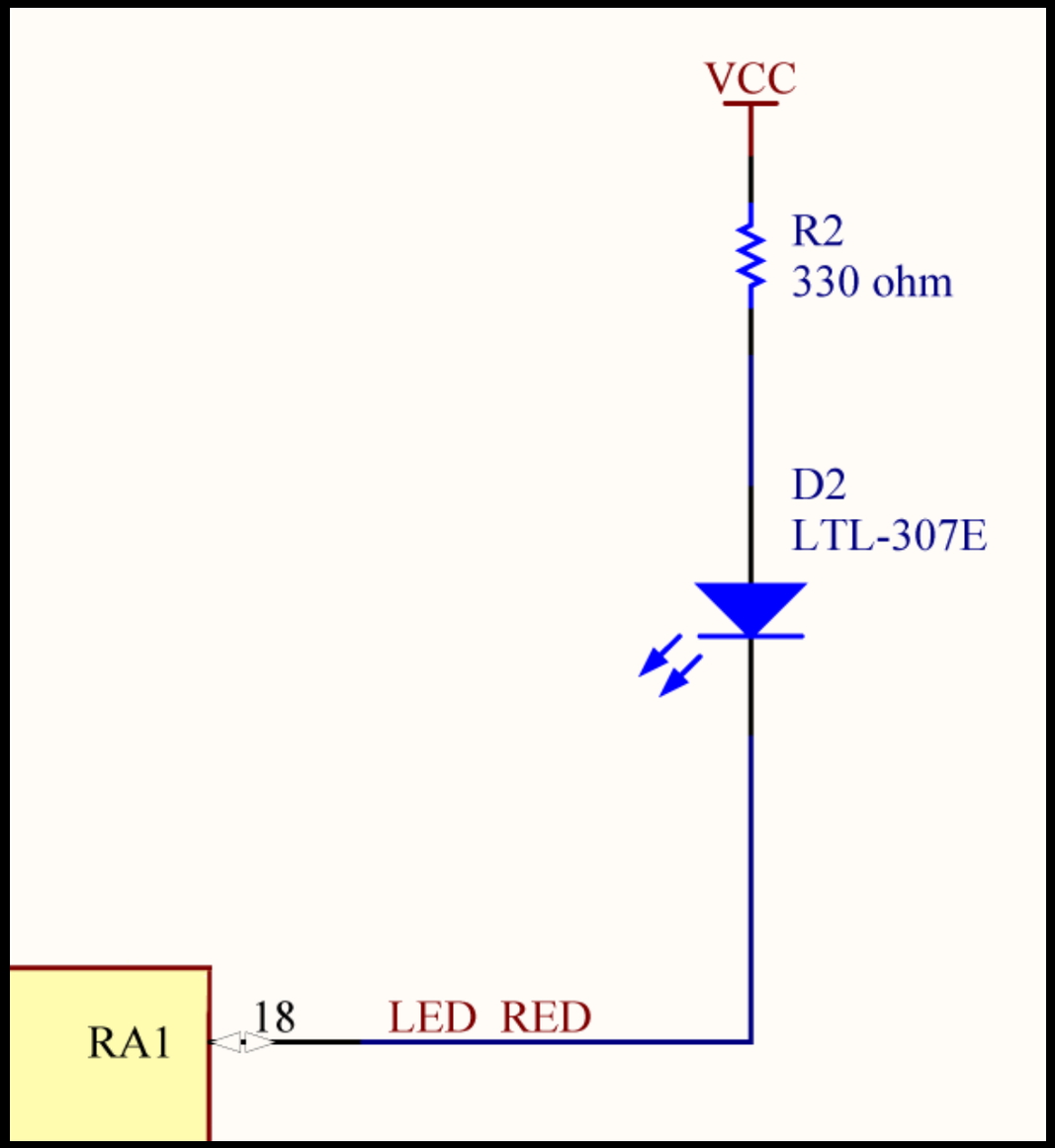
Searching for the Light

- Using LEDs to exfiltrate data
  - Modulate fast enough to not be detected by the human eye
- Optical receiver to convert light into voltage
  - Information Leakage from Optical Emanations (Loughry, Umphress)
  - Canon Hackers Development Kit (CHDK)
  - Demonstration of Hardware Trojans (University of Delaware)
  - Extended Functionality Attacks on IoT Devices: The Case of Smart Lights (Ronen, Shamir)

Playing with Real Hardware!

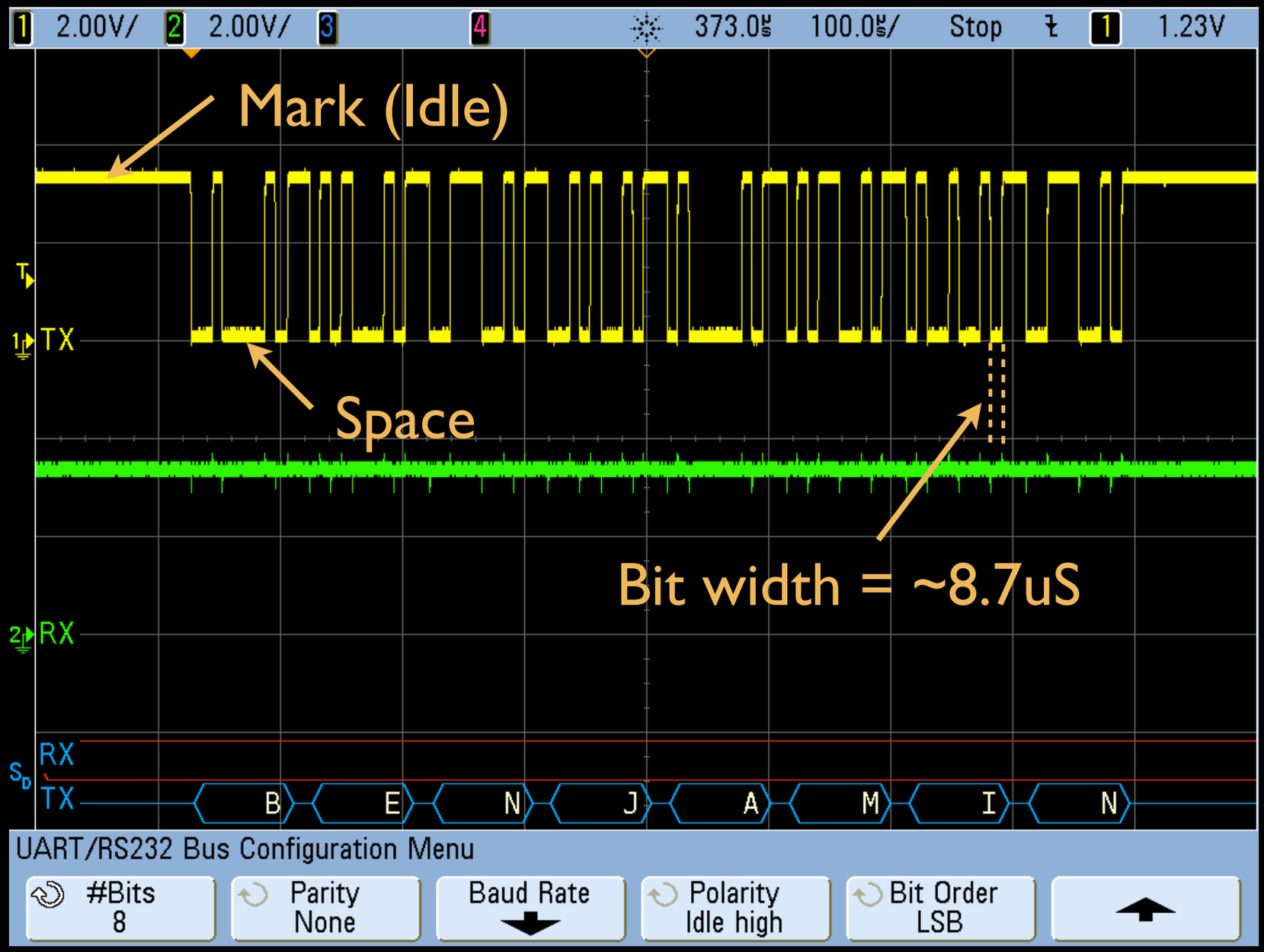
Data Transmission

- Standard LED driver circuit



Data Transmission

- Typically NRZ (Non-Return-to-Zero) coding
  - UART, TOSLINK



Data Transmission

- printf(data)

```
while(1)
{
    #use delay(clock=4000000)
    #use rs232(baud=19200, parity=N, bits=8, xmit=LED_RED, force_sw, stream=LED)
    setup_oscillator(OSC_4MHZ | OSC_INTRC | OSC_PLL_OFF); // increase clock speed
    fprintf(LED, msg_covert); // transmit secret message through the LED
}
```

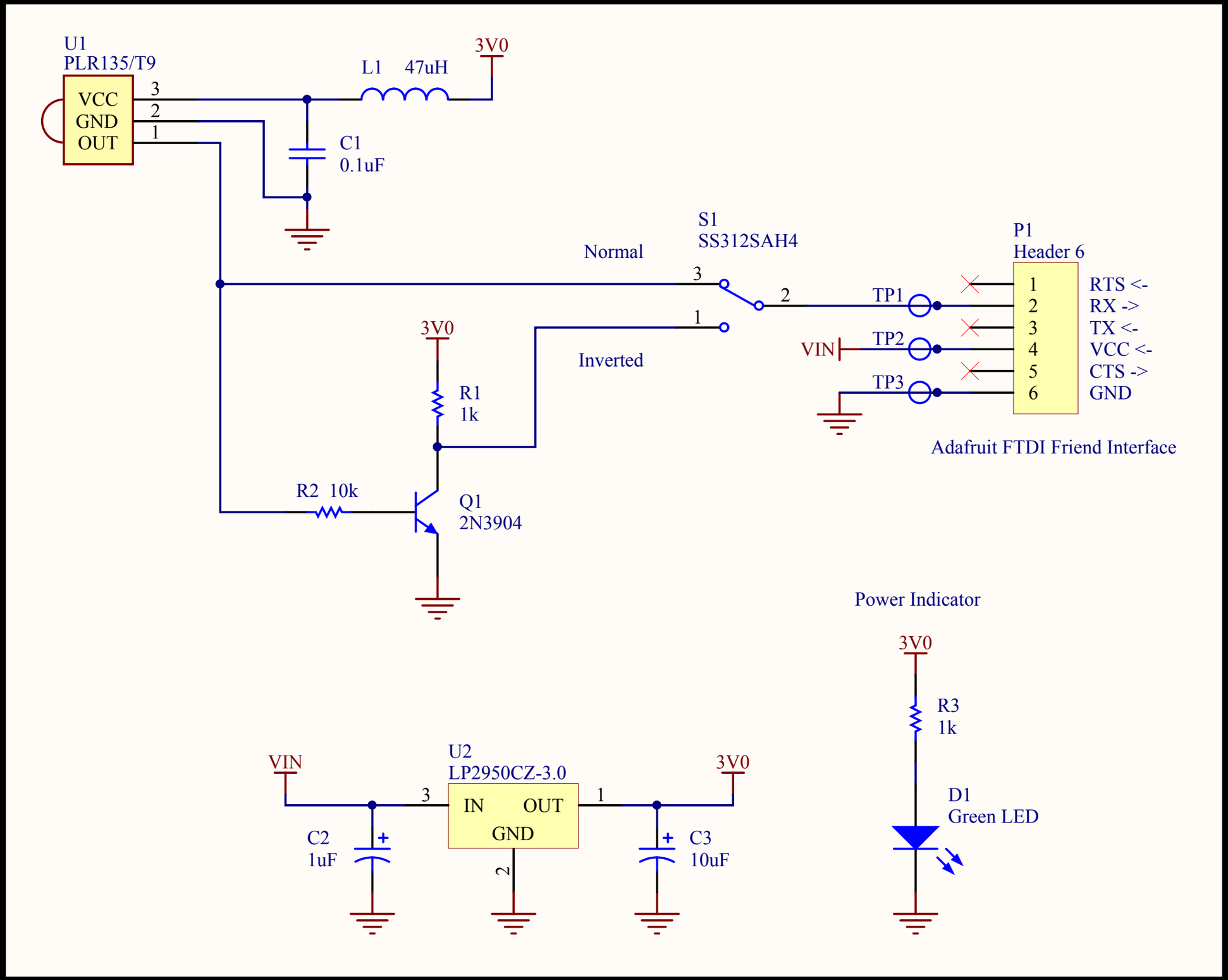
Optical Receiver (Digital)

- Everlight PLR135/T9 Fiber Optic Receiver
  - Handles all optical interfacing, provides TTL output
  - No adjustment/fine-tuning for a particular target signal

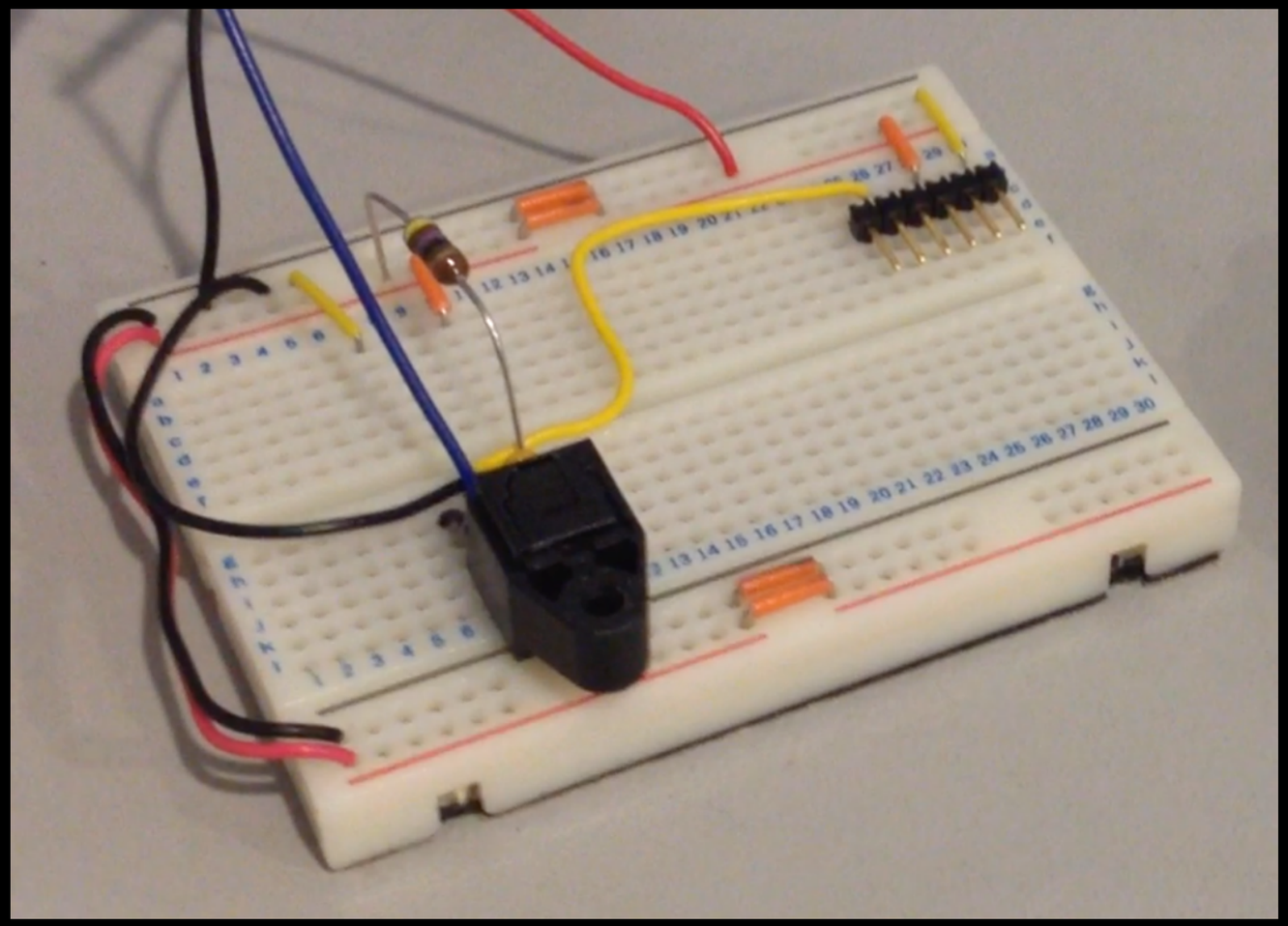
Features

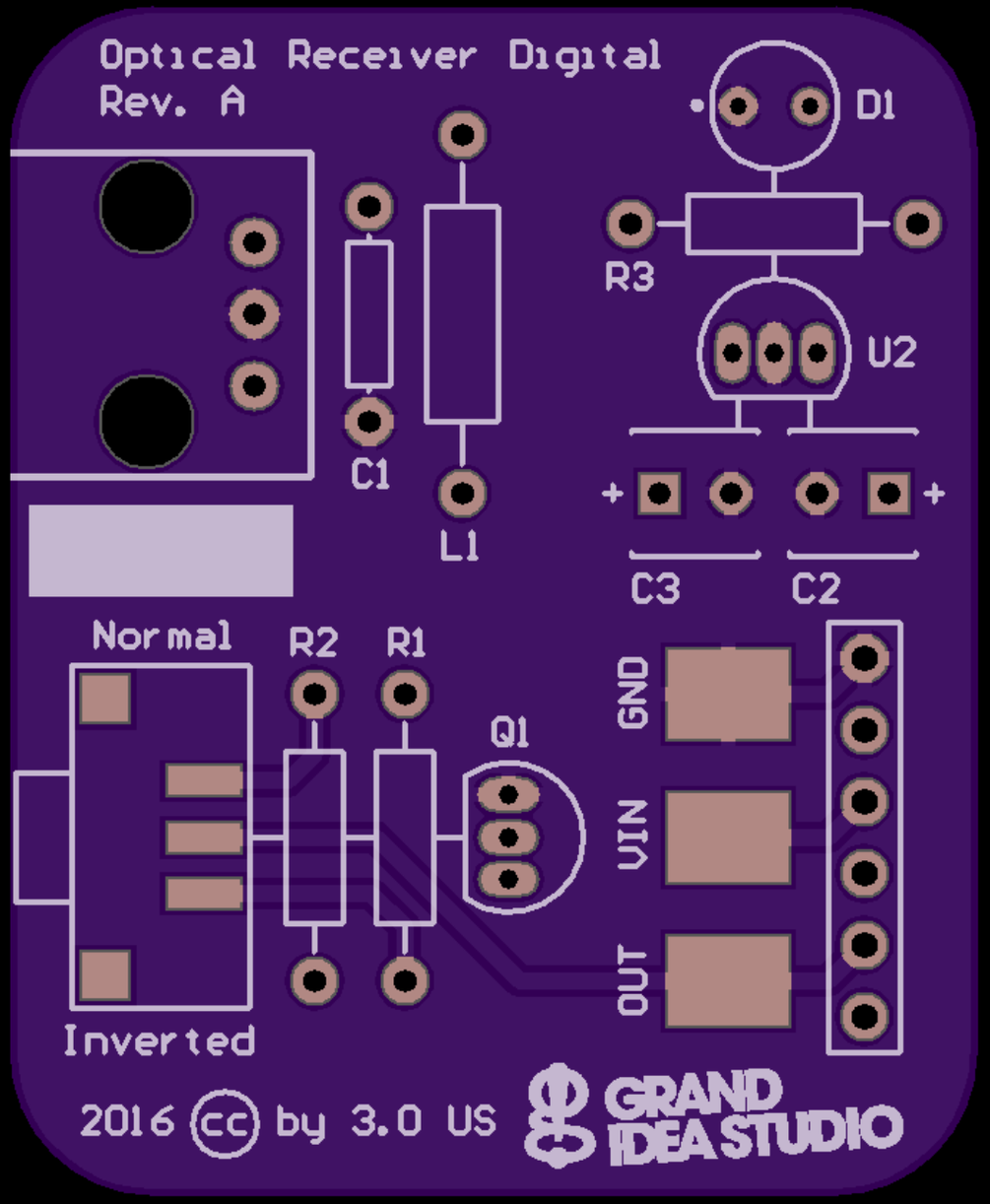
- High PD sensitivity optimized for red light
- Data : NRZ signal
- Low power consumption for extended battery life
- Built-in threshold control for improved noise Margin
- The product itself will remain within RoHS compliant version.
- Receiver sensitivity: up to –27dBm (Min. for 16Mbps)

Optical Receiver (Digital)



Optical Receiver (Digital)

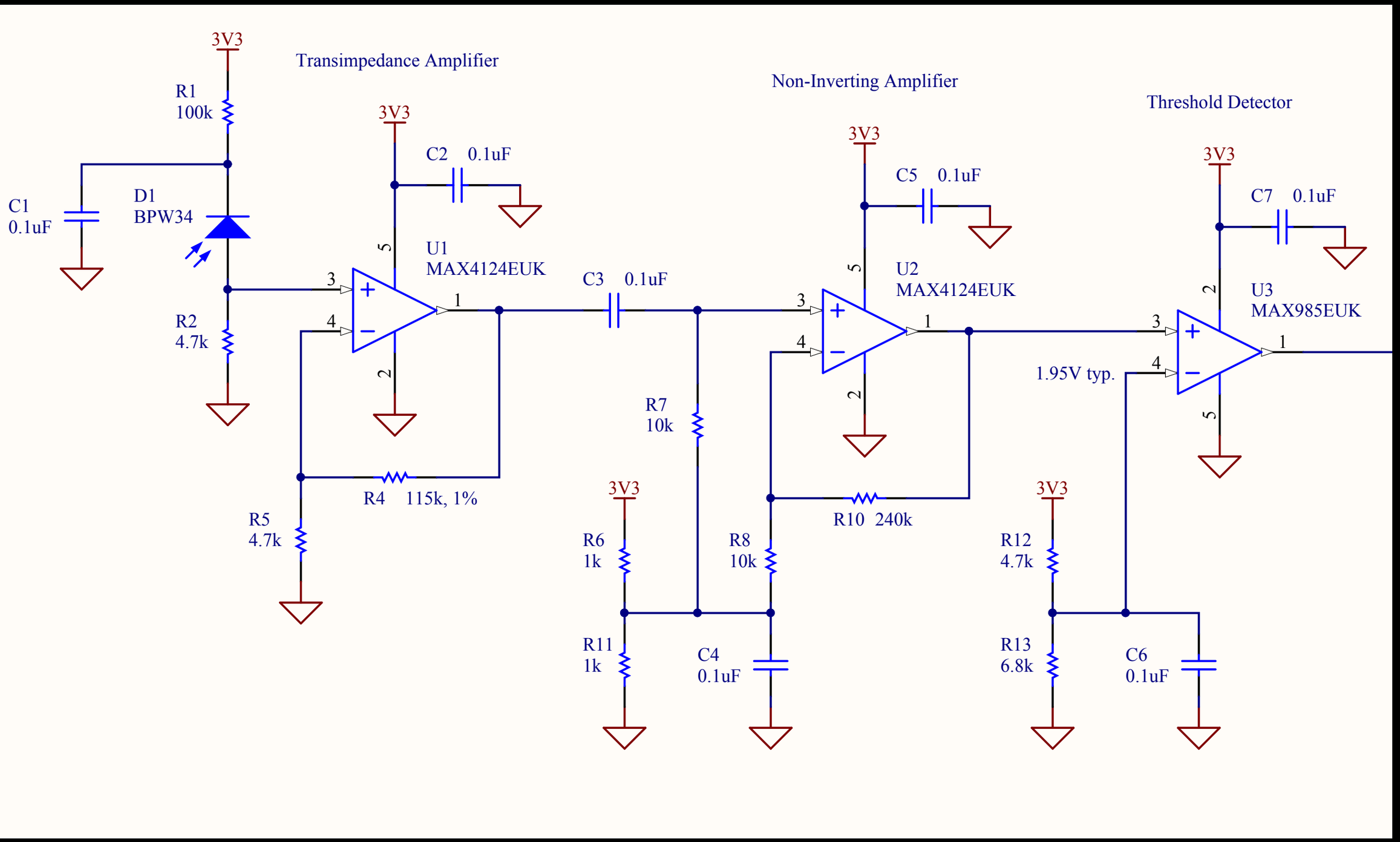




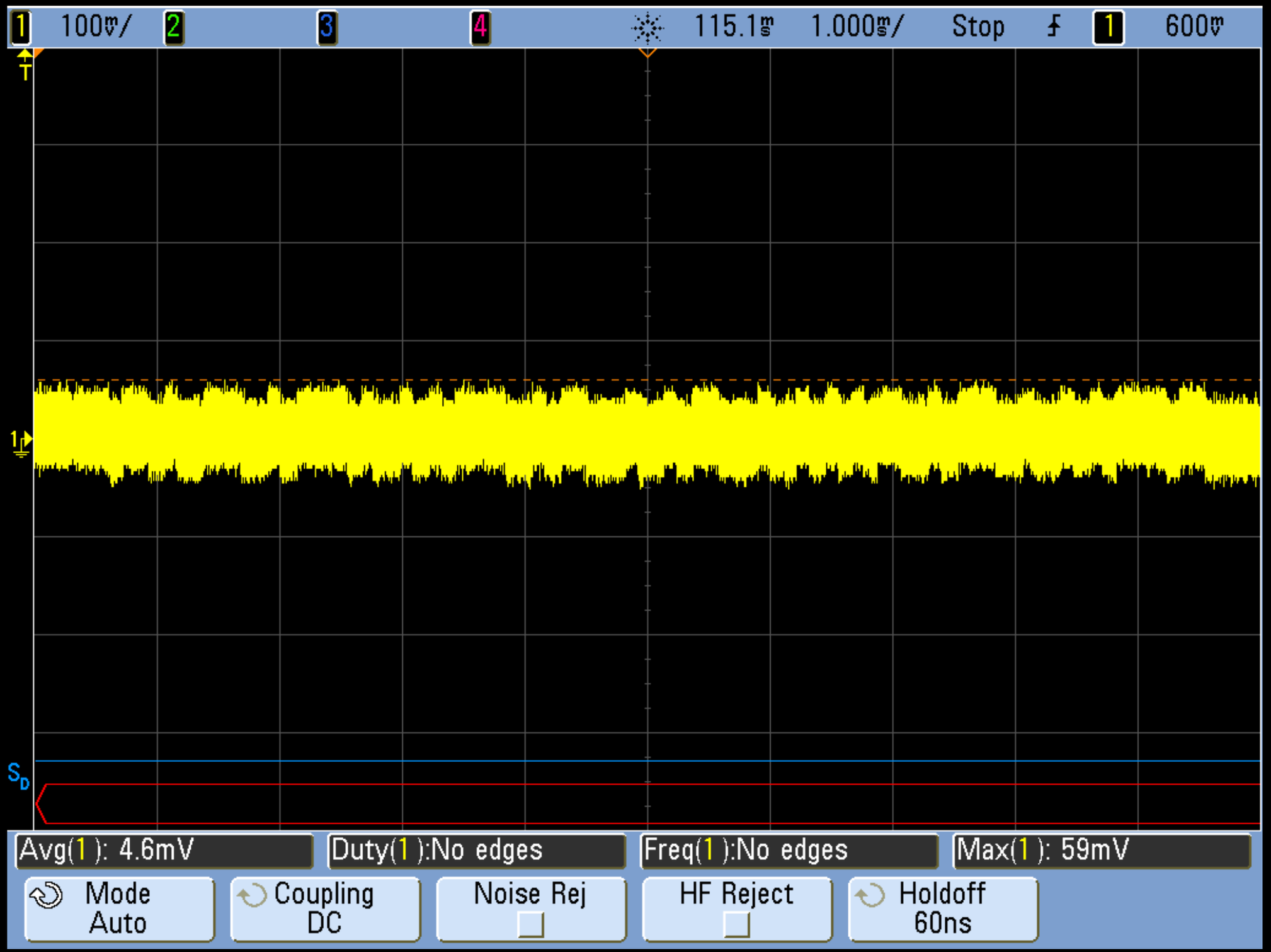
Optical Receiver (Analog)

- Photodiode -> Transimpedance Amplifier -> Comparator
- Adjustment/fine-tuning for a particular target signal
- Not limited to specific binary coding
- Greater risk of extraneous noise/interference
- Based on Maxim Integrated's AN1117: Small Photodiode Receiver Handles Fiber-Optic Data Rates to 800kbps

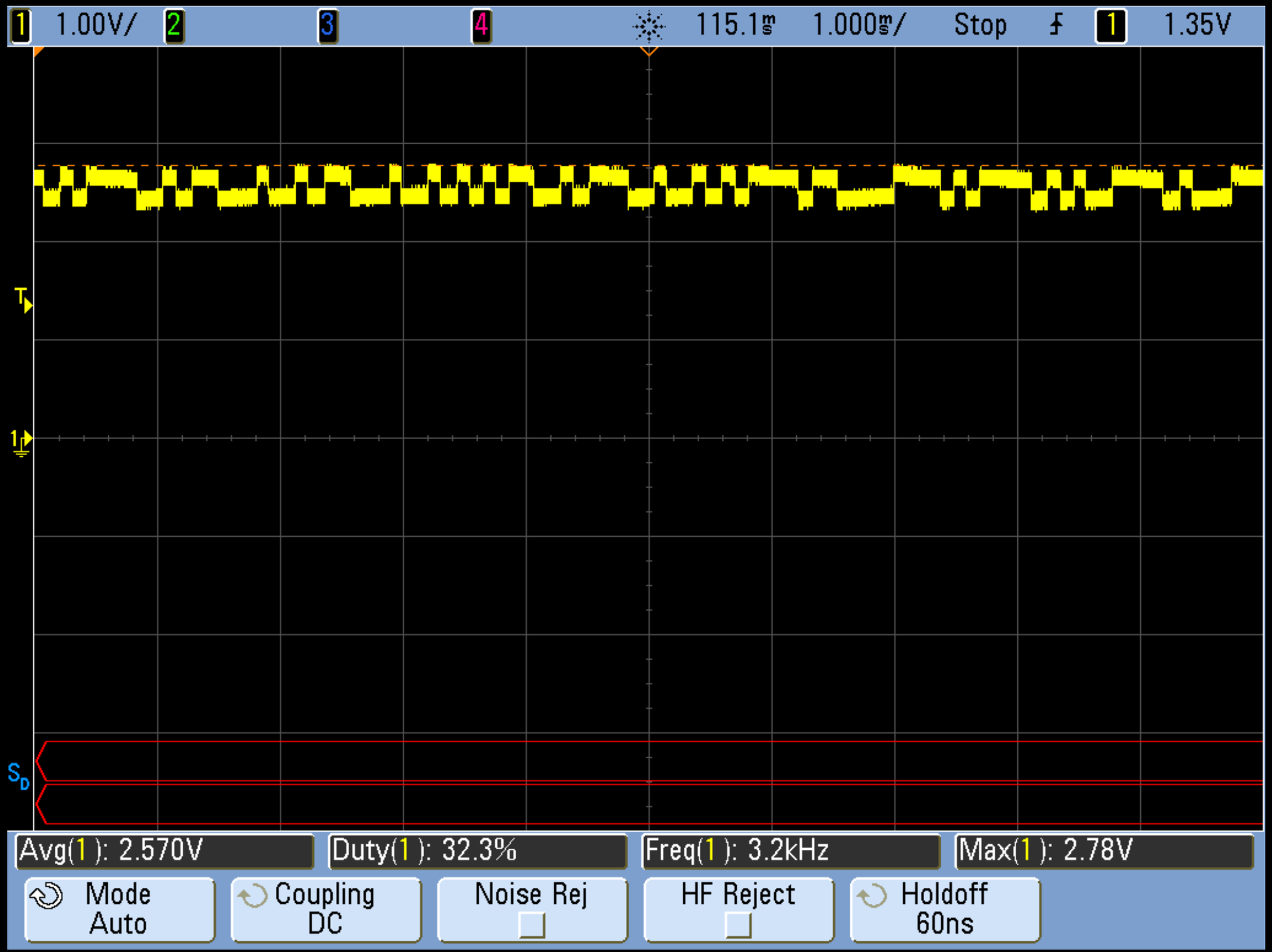
Optical Receiver (Analog)



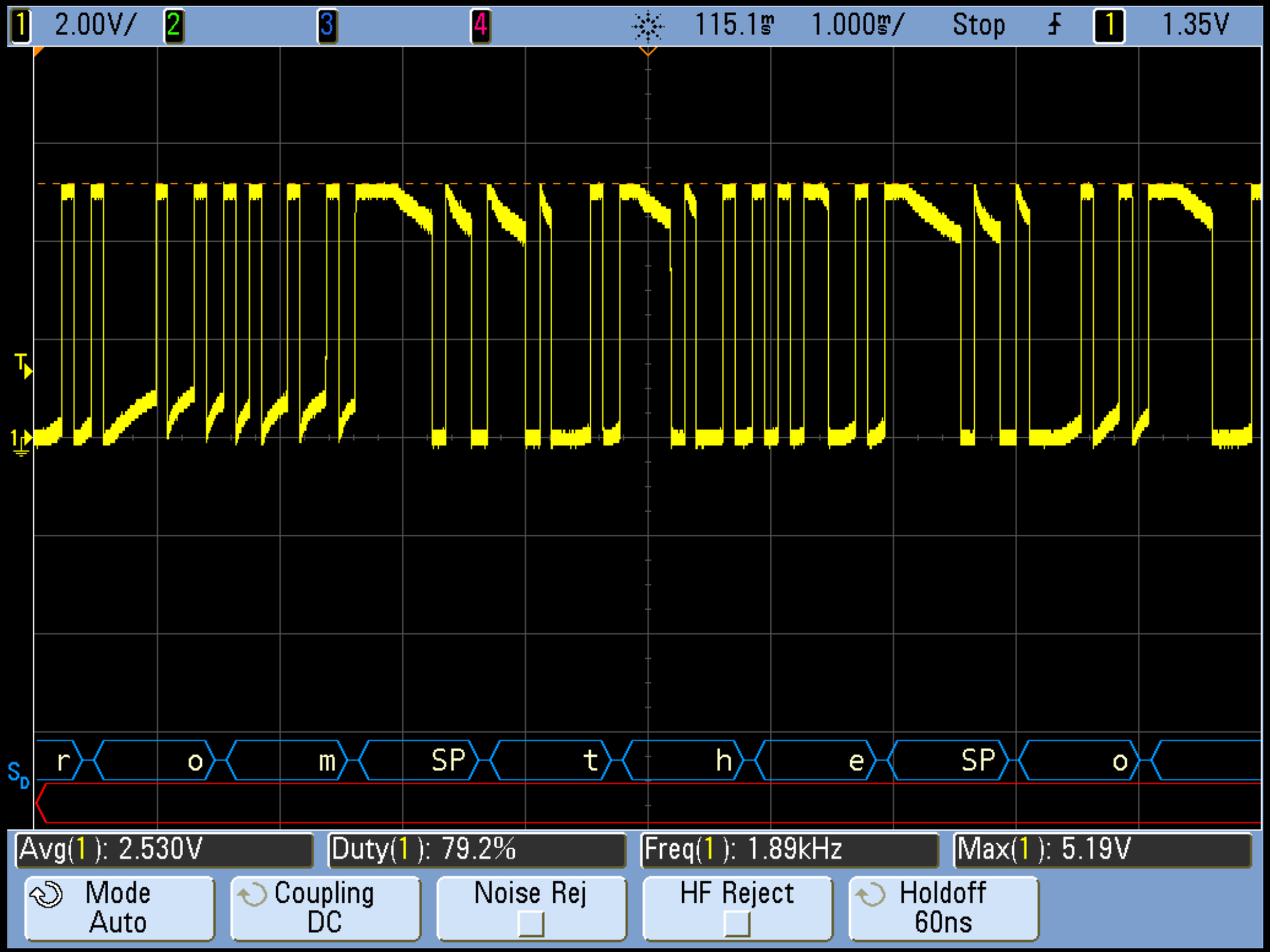
Optical Receiver (Analog)



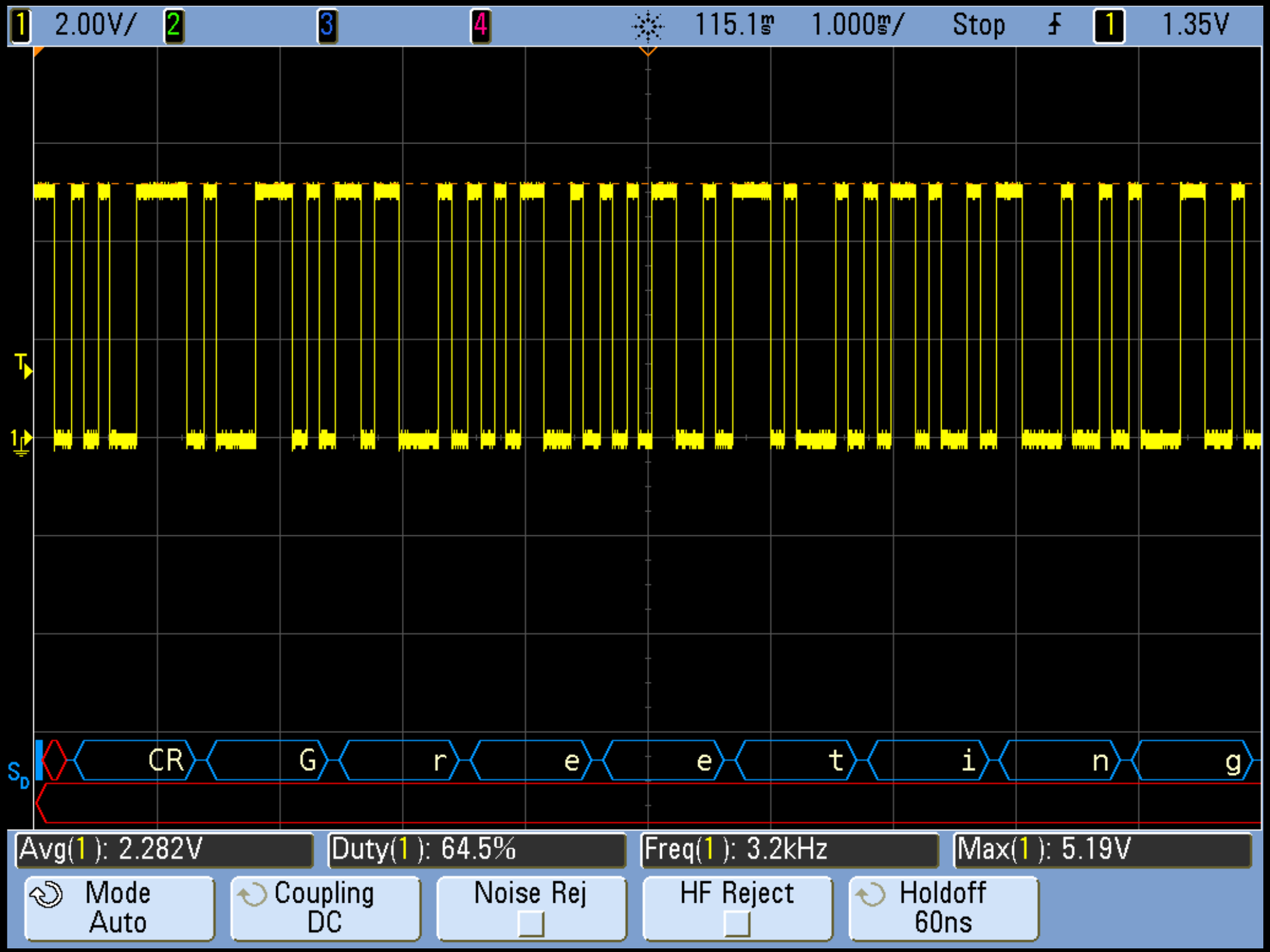
Optical Receiver (Analog)



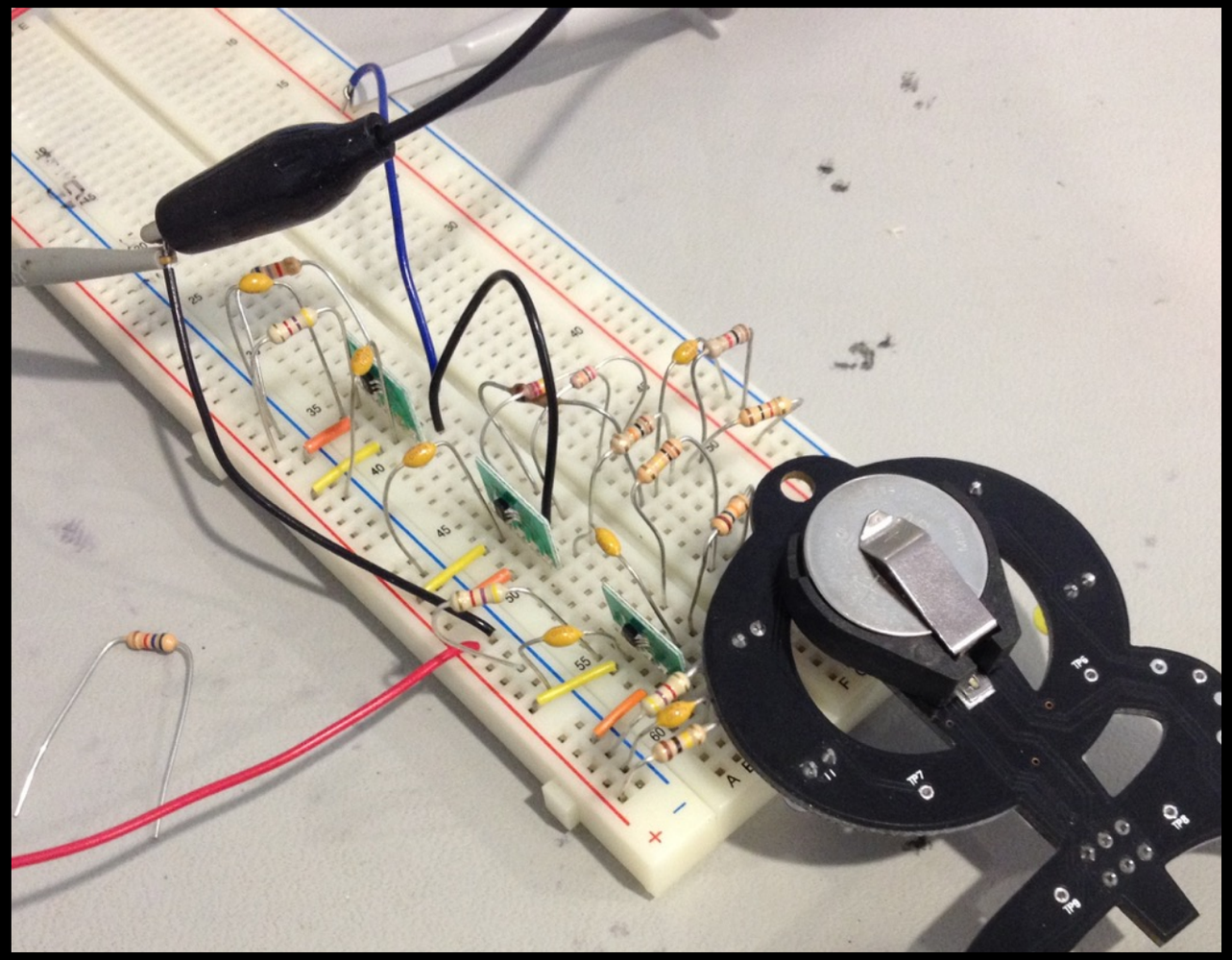
Optical Receiver (Analog)

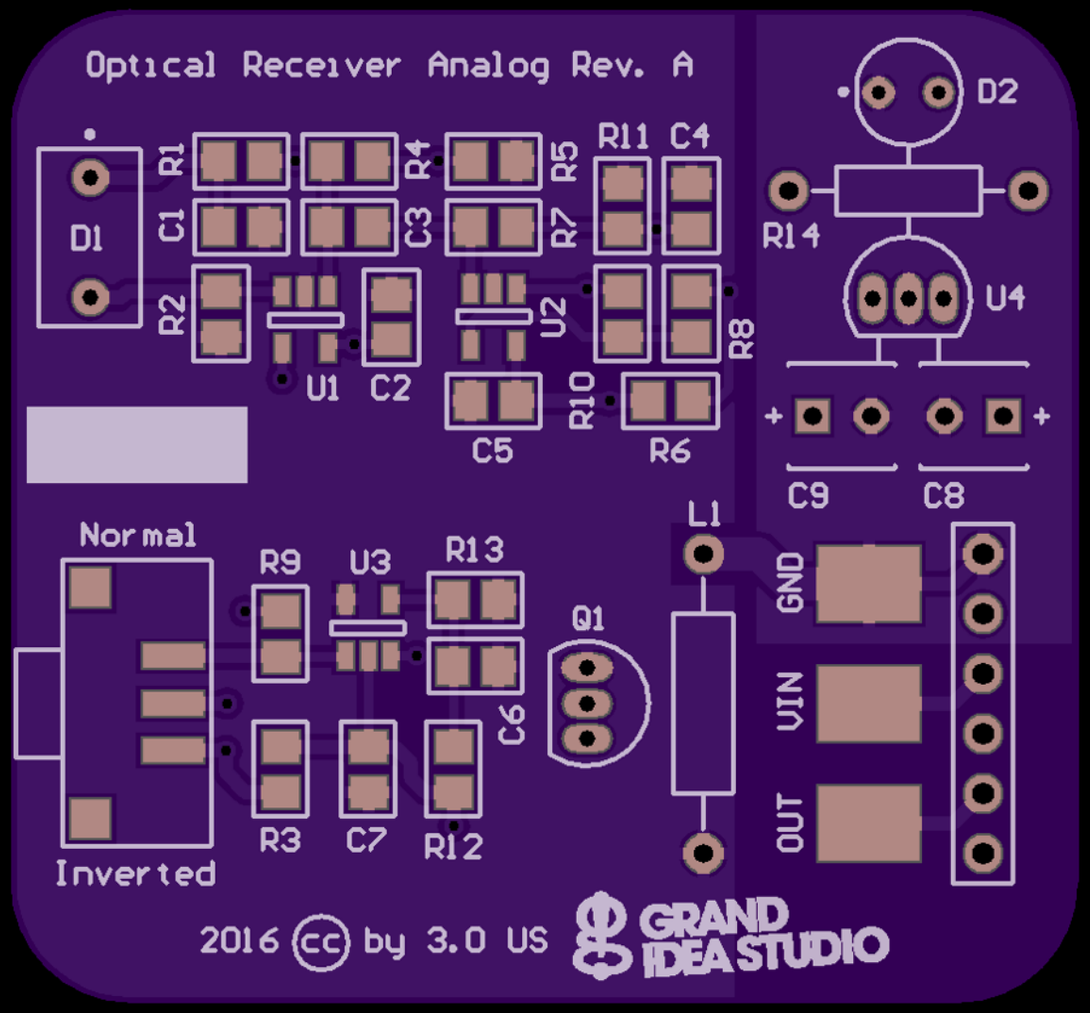


Optical Receiver (Analog)



Optical Receiver (Analog)





Possible Detection Methods

- Optical receivers (as described here)
- High speed camera focused on target LED
  - May be difficult to differentiate between legitimate PWM and illegitimate data exfiltration
- Firmware/source code/RTL analysis, diff against known-good image

Build Your Own

- www.grandideastudio.com/portfolio/optical-covert-channels

  *** Schematic, BOM, Gerber plots, assembly drawing

- http://oshpark.com/profiles/joegrand

  *** Bare boards

THANKS FOR YOUR TIME!