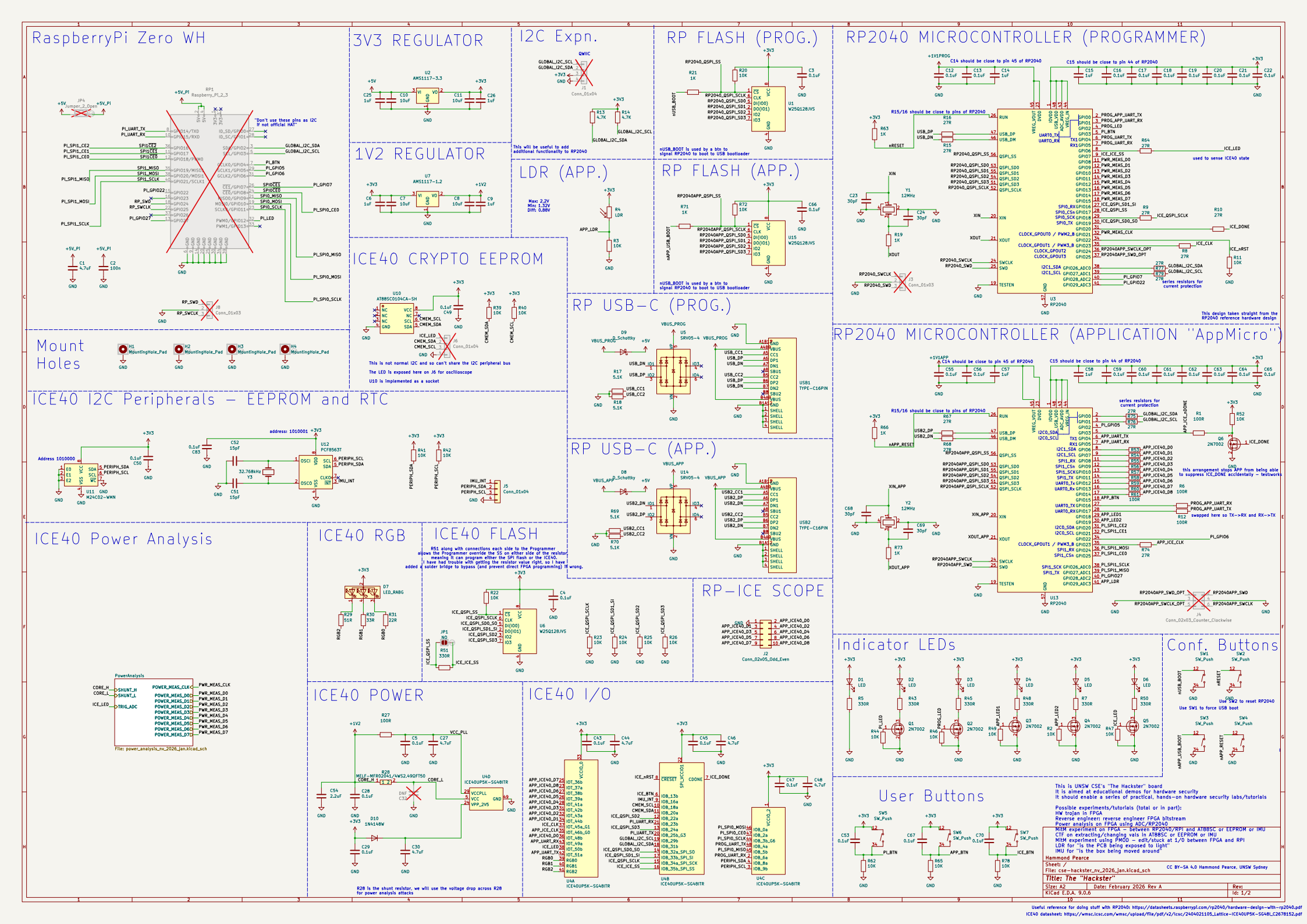
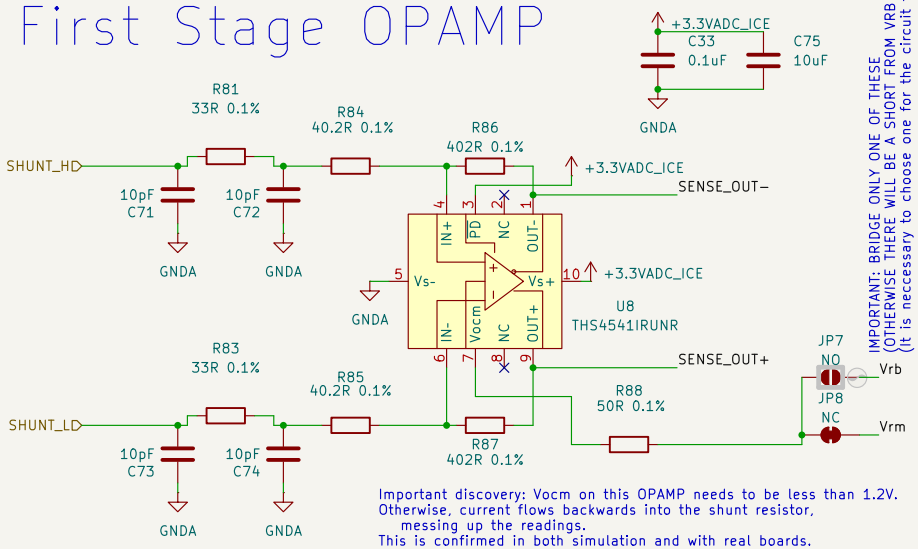

RaspberryPi Zero WH
3V3 REGULATOR
I2C Expn.
RP FLASH (PROG.)
RP2040 MICROCONTROLLER (PROGRAMMER)
1V2 REGULATOR
LDR (APP.)
RP FLASH (APP.)
ICE40 CRYPTO EEPROM
RP USB-C (PROG.)
RP2040 MICROCONTROLLER (APPLICATION "AppMicro")
Mount Holes
ICE40 I2C Peripherals - EEPROM and RTC
RP USB-C (APP.)
ICE40 Power Analysis
ICE40 RGB
ICE40 FLASH
RP-ICE SCOPE
Indicator LEDs
Conf. Buttons
ICE40 POWER
ICE40 I/O
User Buttons
This is UNSW CSE's "The Hackster" board
It is aimed at educational demos for hardware security
It should enable a series of practical, hands-on hardware security labs/tutorials
Possible experiments/tutorials (total or in part):
HW trojan in FPGA
Reverse engineer: reverse engineer FPGA bitstream
Power analysis on FPGA using ADC/RP2040
MiTM experiment on FPGA - between RP2040/RPi and AT88SC or EEPROM or IMU
CTF on extracting/changing vals in AT88SC or EEPROM or IMU
MiTM experiment using PMOD - edit/stuck at 1/0 between FPGA and RPi
LDR for "is the PCB being exposed to light"
IMU for "is the box being moved around"
Hammond Pearce
Sheet: /
File: cse-hackster_nv_2026_jan.kicad_sch
CC BY-SA 4.0 Hammond Pearce, UNSW Sydney
Title: The "Hackster"
Size: A2
Date: February 2026 Rev A
Rev:
KiCad E.D.A. 9.0.6
Id: 1/2
Useful reference for doing stuff with RP2040: https://datasheets.raspberrypi.com/rp2040/hardware-design-with-rp2040.pdf
ICE40 datasheet: https://wmsc.lcsc.com/wmsc/upload/file/pdf/v2/lcsc/2404021105_Lattice-ICE40UP5K-SG48I_C2678152.pdf

ICE40 Power Analysis — First Stage OPAMP



IMPORTANT: BRIDGE ONLY ONE OF THESE
(OTHERWISE THERE WILL BE A SHORT FROM VRB TO VRM)
(It is neccessary to choose one for the circuit to function)

Important discovery: Vocm on this OPAMP needs to be less than 1.2V.
Otherwise, current flows backwards into the shunt resistor,
messing up the readings.
This is confirmed in both simulation and with real boards.

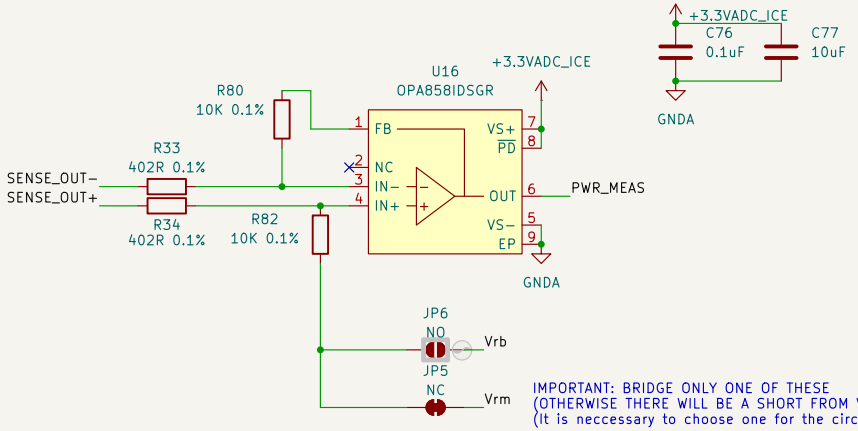
We estimate the transient to be about 0.5mA when running 4 AES S-Boxes.
With a 2.490hm shunt (R28), we get 1.245mV of transient Voltage.

Using THS4541 as the first gain stage, we will do x10 gain to get 12.45mV of transient while re-centering it around Vrm
This is a DFA to give us a strong CMRR, and avoiding extra level shifting thanks to the Vocm input.

The second opamp stage, using OPA858, gives us an additional x24.8 gain (giving us x248 overall).
This takes our 12.45mV transient to ~308mV transient (should be very detectable!)
I also design it so we can offset the second stage from Vrm or Vrb.

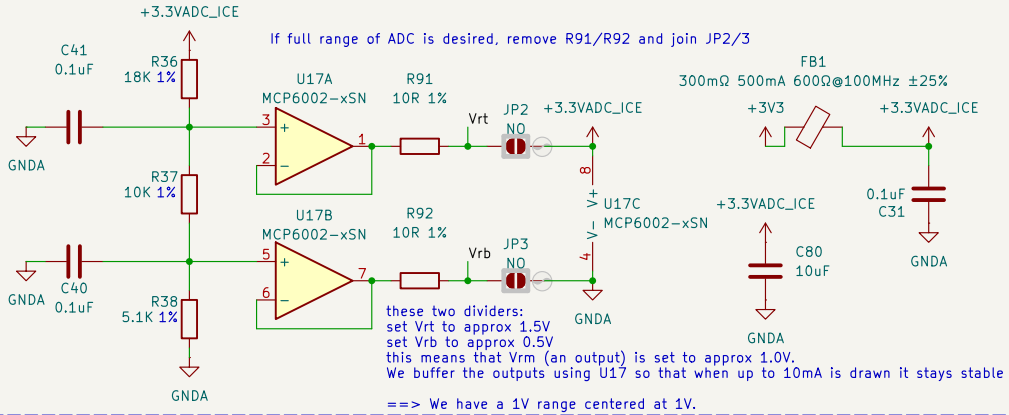
Finally, the ADC has a 1V range around 1V (Should go from 0.5V to 1.5V).
0.5V + 0.3V is only 0.9V, leaving us a fair amount of headroom (about 60% left)
Given that these measurements are for just 4 S-Boxes, this gives some headroom for larger designs.
Additionally, we provide an SMA connector with the sample at it, so we could in theory use an o-scope instead.

Second Stage OPAMP



IMPORTANT: BRIDGE ONLY ONE OF THESE
(OTHERWISE THERE WILL BE A SHORT FROM VRB TO VRM)
(It is neccessary to choose one for the circuit to function)

Power Rails/ Voltage Ref. Generator

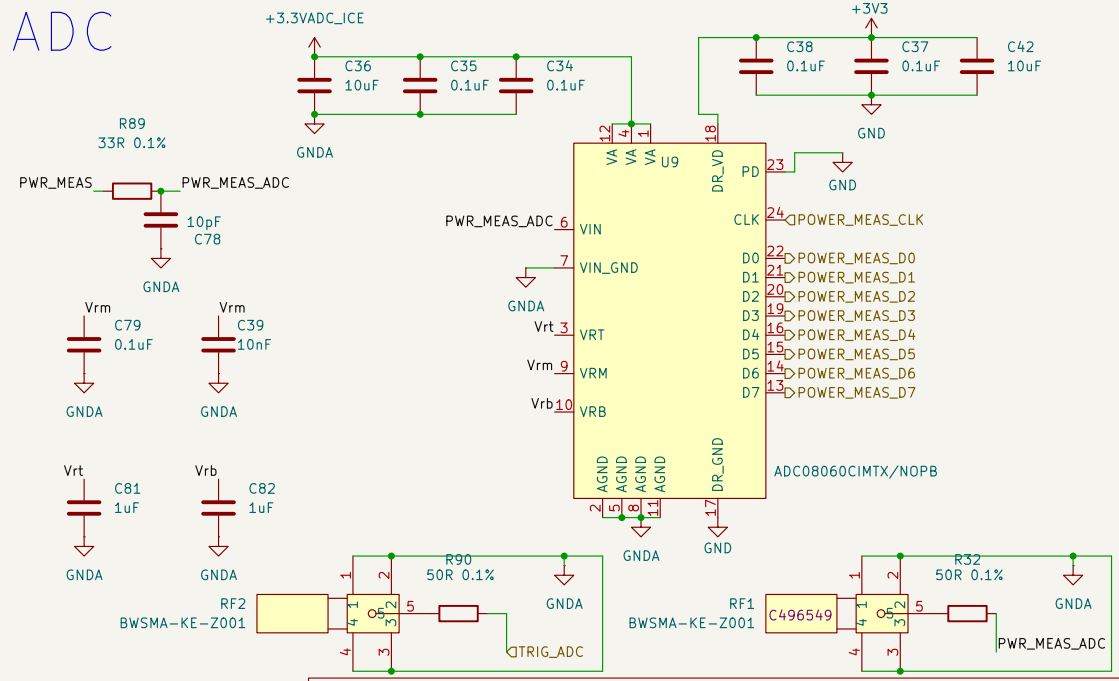


If full range of ADC is desired, remove R91/R92 and join JP2/3

these two dividers:
set Vrt to approx 1.5V
set Vrb to approx 0.5V
this means that Vrm (an output) is set to approx 1.0V.
We buffer the outputs using U17 so that when up to 10mA is drawn it stays stable

==> We have a 1V range centered at 1V.

ADC



Sheet: /PowerAnalysis/
File: power_analysis_nv_2026_jan.kicad_sch

Title: Hackster Power Analysis

Size: A4 | Date: | **Rev:**
KiCad E.D.A. 9.0.6 | Id: 2/2