PropLANE

Kind of keeping the NSA from watching you pee

Introduction

- The guys up here
  - Mark Carey (phorkus)
  - Russ Rogers (russr)
  - Ryan Clarke (L0stboy)
  - Rob Bathurst (evilrob)
- Guys not up here
  - You

History of Crypto Part I

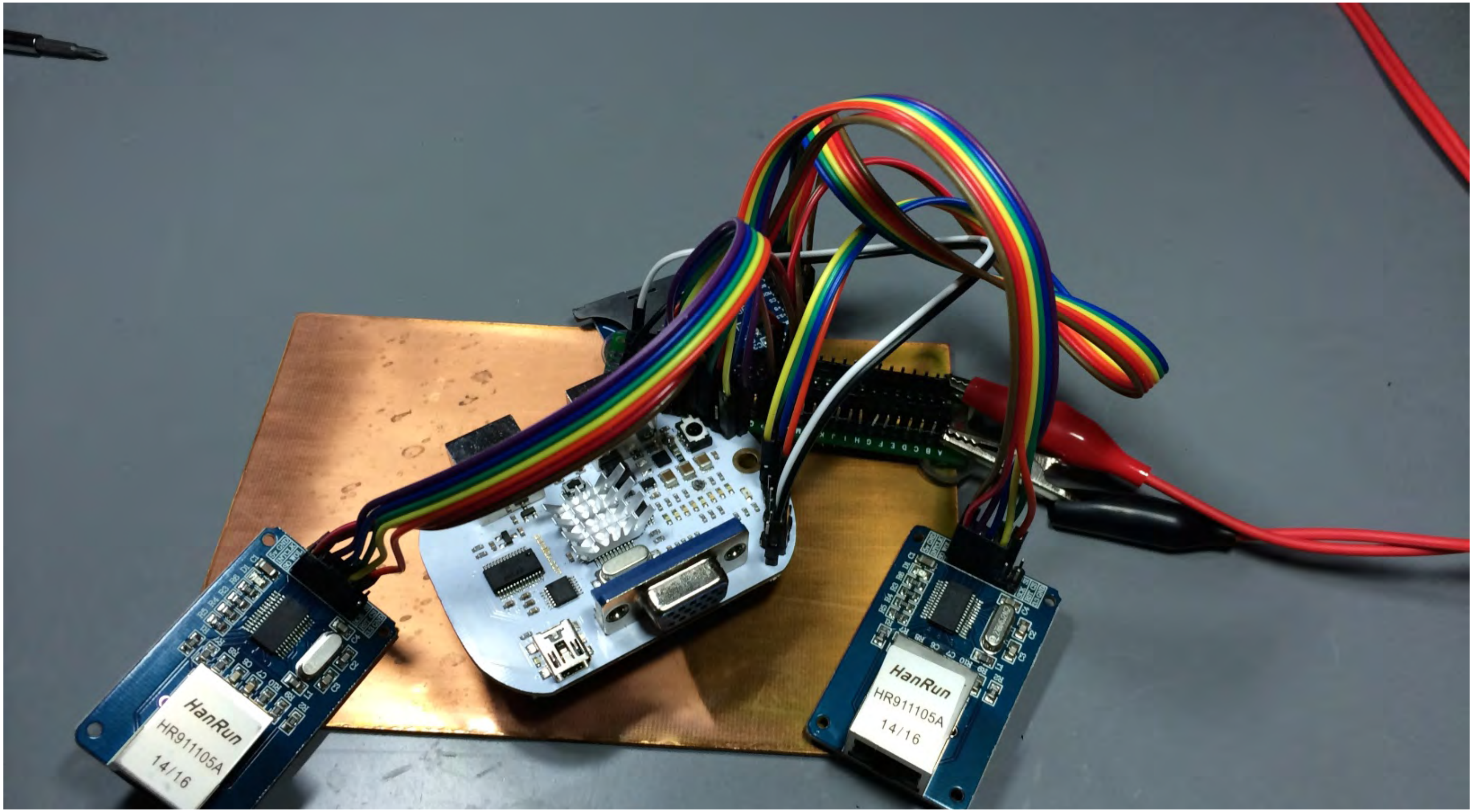
- Scytale
- Caesar Cipher
- One Time Pad (OTP)
- Enigma Machine
- SIGABA
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

Recent Things in History

- The NSA vacuum
- Is TOR safe!?!?!
- The Freenet Project

The Project

The Pile



The PropLANE

- The Idea!
  - .gov style network protection for the masses
- Why did we do this?
  - we too like to keep our shit, our shit, and just our shit
- How did we do this?
  - DARPA CFT

The Parts Part I

- DC 20 Badge
  - Parallax Propeller Chip
  - 16 User I/O Pins
  - SPI Boot ROM
  - TTL Serial-to-USB
  - Infrared Transceiver

The Parts Part II

- Additional Items
  - Ethernet Transceiver
    - Microchip ENC28J60
    - 3.3/5v
    - 8k Static Ram Buffer
    - If you don't use this, you will have to write your own driver
  - SD Card (keystore)
    - Almost any SD card will work

The Software

- Spin
  - “high level” programming language
  - byte code interpreter
  - learn.parallax.com
- PASM
  - Propeller Assembly
  - Faster
  - pPropellerSim/GEAR

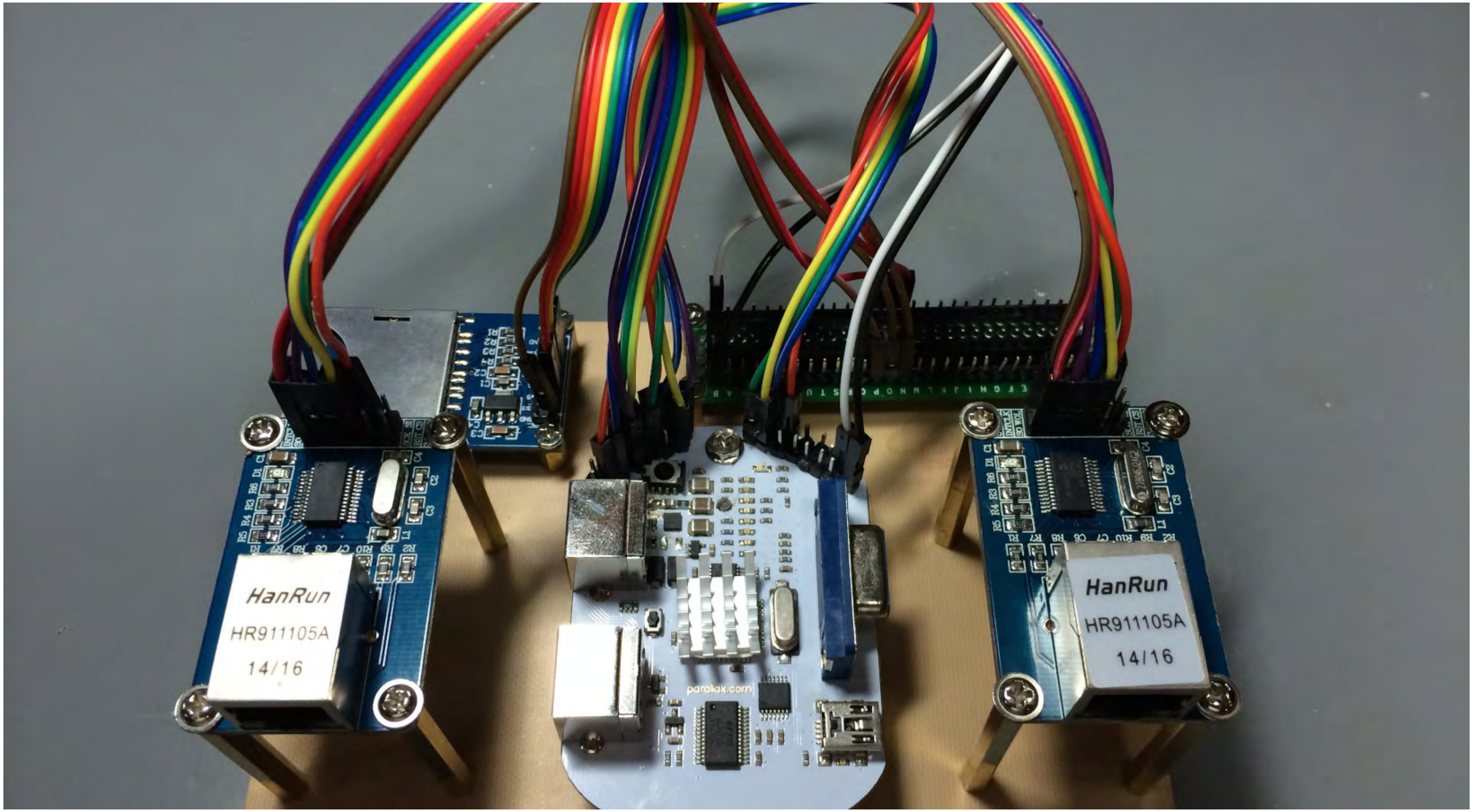
Fair Warning

- Synthesized SPI using specialized COG instructions
- Transparent bridging
- Small key size (128 vs 256) due to size constraints

Warning About Crypto

- Why crypto works
  - Hash vs Encryption
- Crypto can be defeated
  - Losing your symmetric key
  - Compromised PKI
  - Brute Force
  - Poor Implimentation

Money Shot



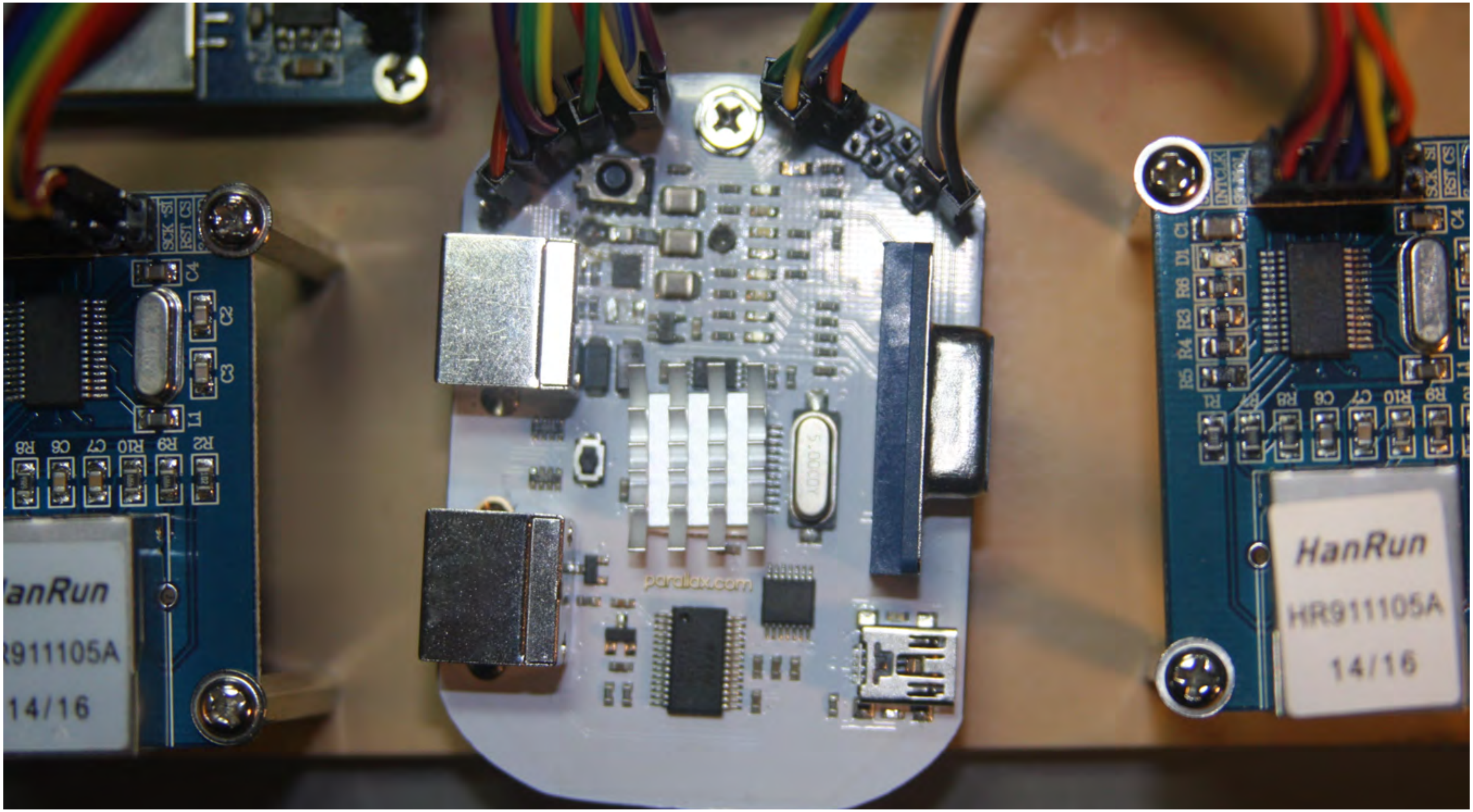
The Problem

Approach

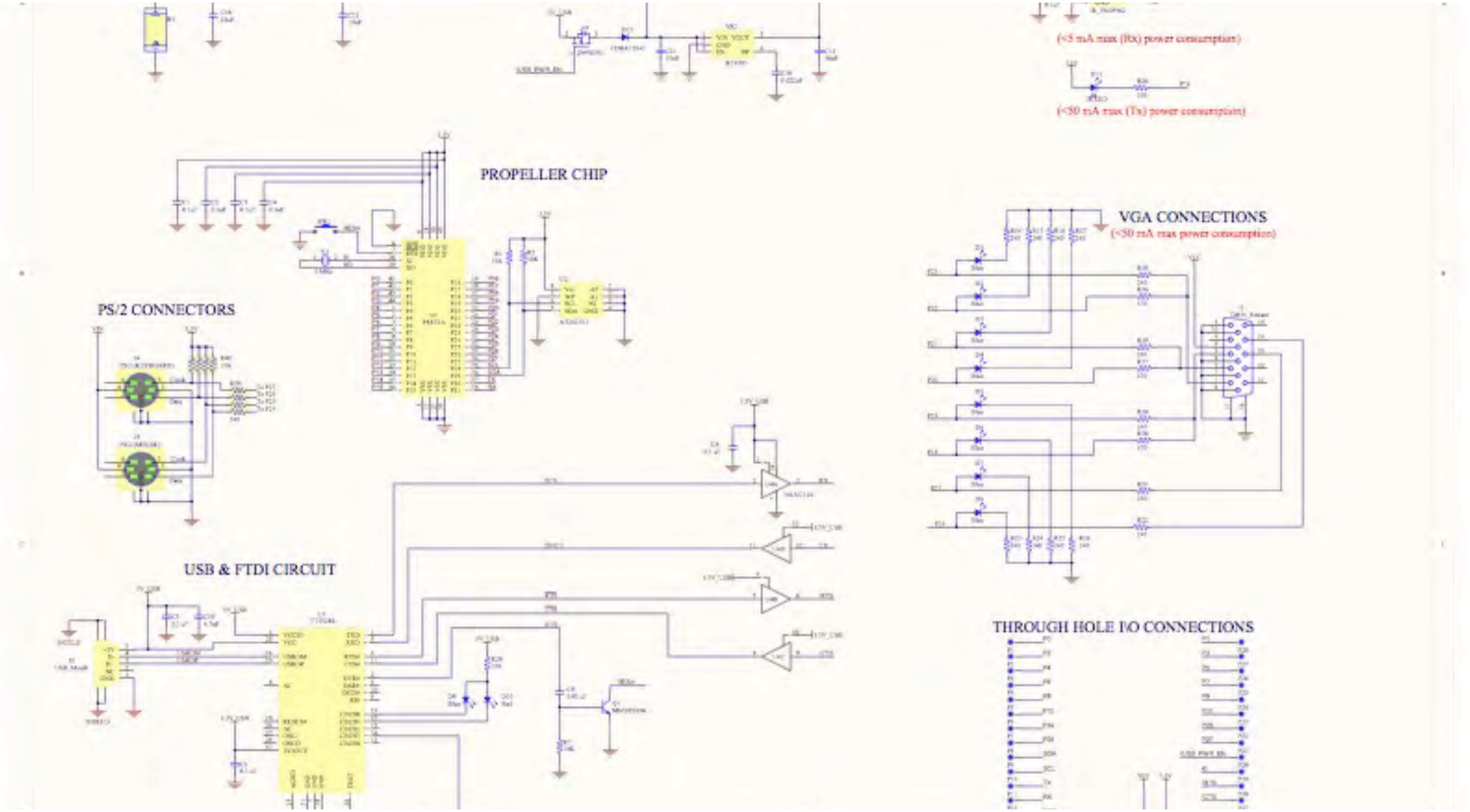
- Cheap
  - Propeller
  - Arm
- Fast-ish
  - Propeller (not so fast)
  - ARM (can be fast)
  - FPGA (screaming fast)
- Easy to use
  - Simple key exchange
  - ON/OFF switch

The Badge

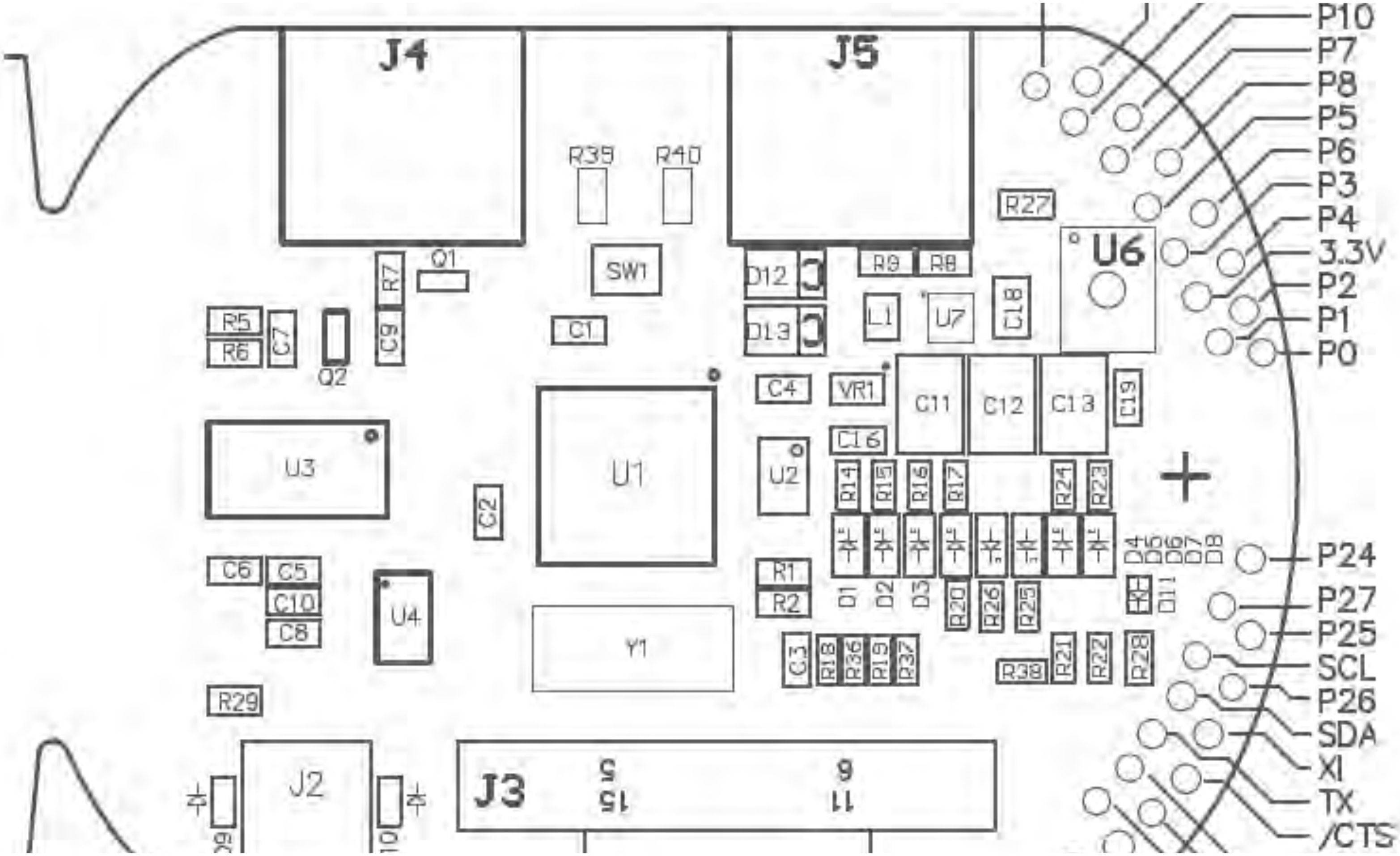
DC 20 Badge



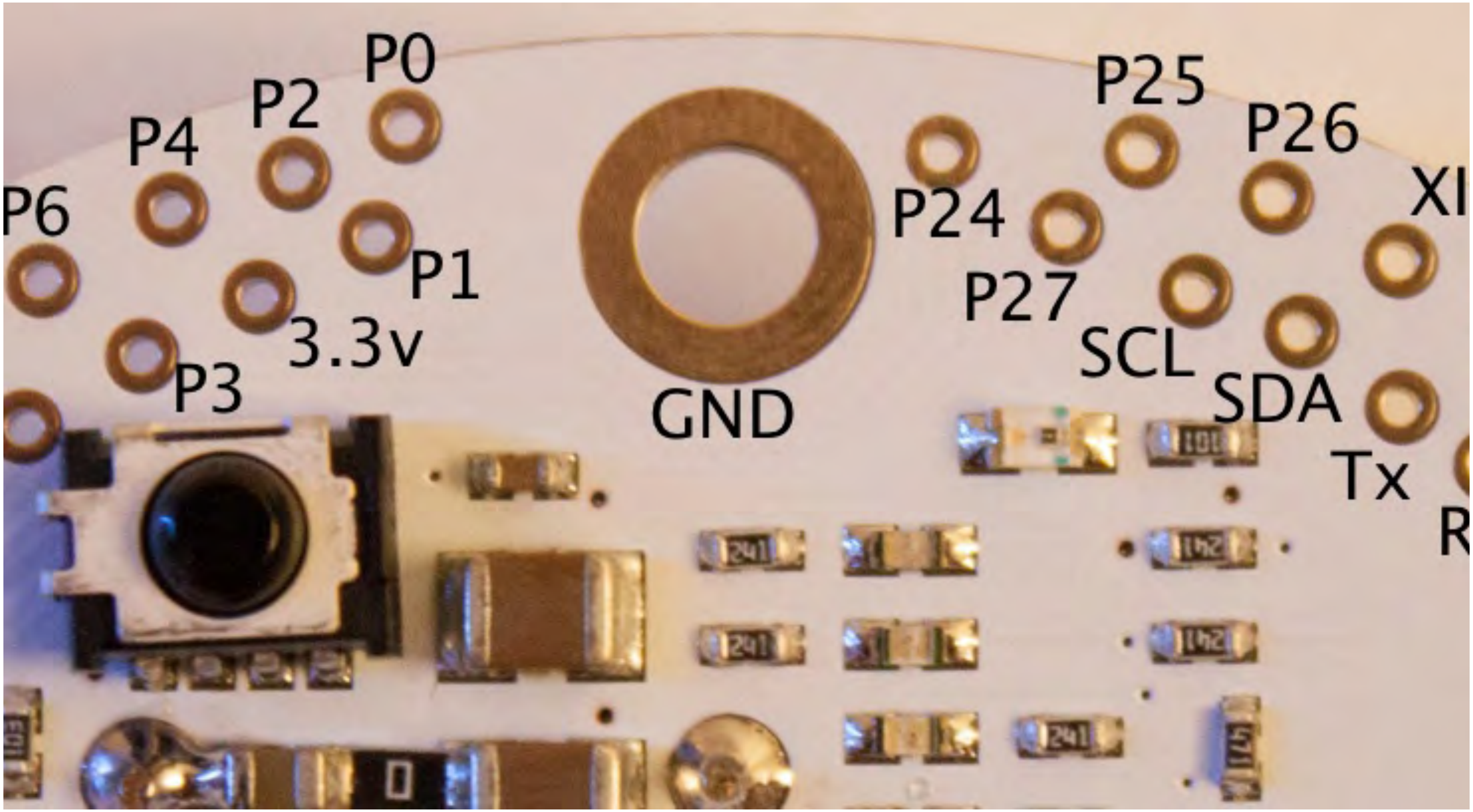
Badge Schematic


(<5 mA max (Rx) power consumption)
(<50 mA max (Tx) power consumption)
PROPELLER CHIP
VGA CONNECTIONS
(<50 mA max power consumption)
PS/2 CONNECTORS
USB & FTDI CIRCUIT
THROUGH HOLE I/O CONNECTIONS

Pinout


J4
J5
P10
P7
P8
P5
P6
P3
P4
3.3V
P2
P1
P0
R39
R40
R27
U6
Q1
R7
SW1
D12
D13
R9
R8
L1
U7
C18
R5
R6
C7
Q2
C9
C1
C4
VR1
C11
C12
C13
C19
C16
U3
U1
U2
C2
R14
R15
R16
R17
R24
R23
D1
D2
D3
D4
D5
D6
D7
D8
D11
P24
P27
P25
SCL
P26
SDA
XI
TX
/CTS
C6
C5
C10
C8
U4
R1
R2
Y1
R20
R26
R25
C3
R18
R36
R19
R37
R38
R21
R22
R28
R29
J2
J3
5
15
6
11

Pinout



PropLANE Software

How a Propeller Works

- Cogs
- Jobs
- Spin/PASM
- What if I want to port it?

The Crypto Cog

- Encrypt Cog
- Decrypt Cog
- Speed Test
- Basic Sequence
  - Packet In
  - Mem Copy
  - Decrypt
  - Read/Write
  - Encrypt
  - Mem Copy
  - Packet Out

The Network Cog

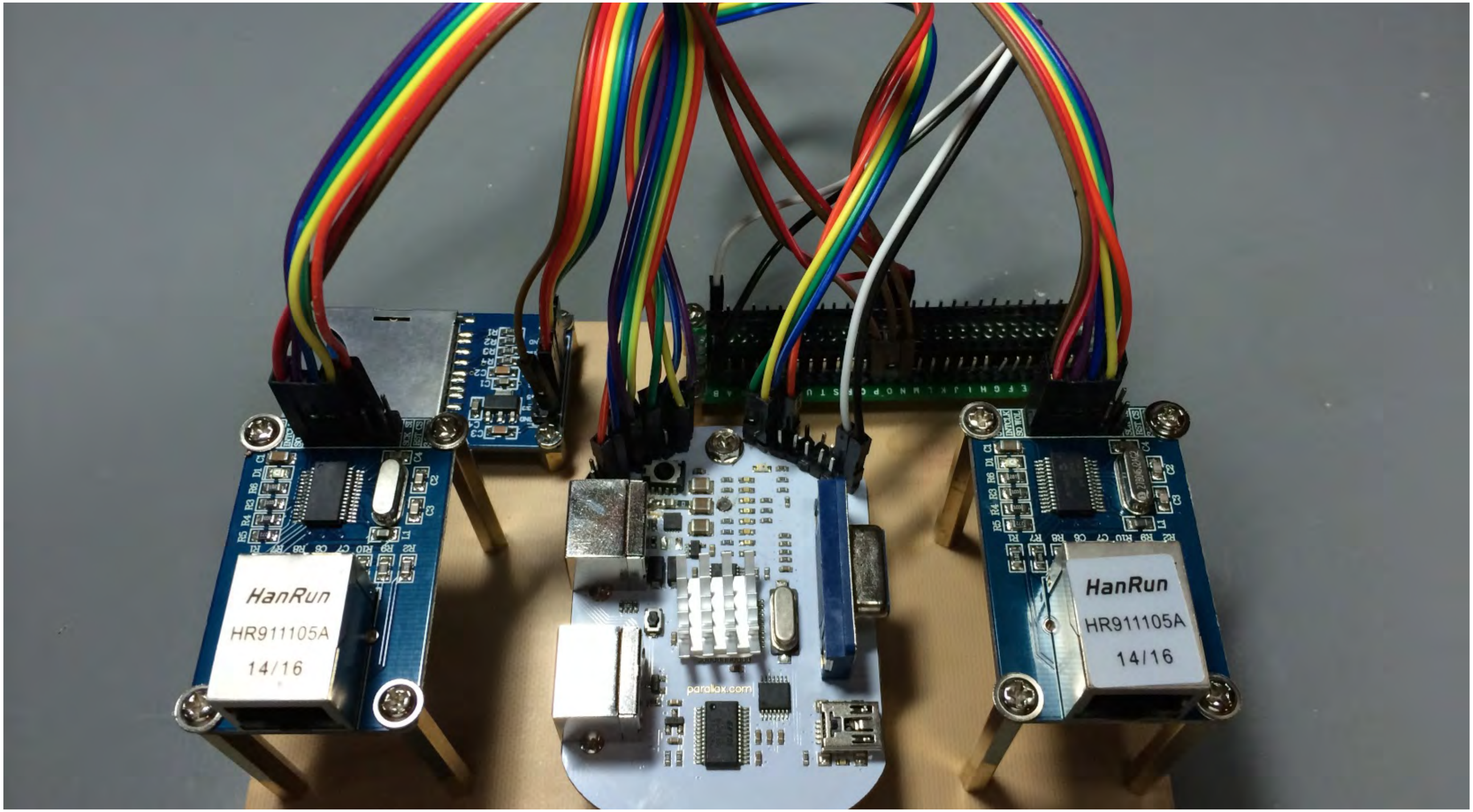
- Network Comms Design
  - 2 SPI Cogs
  - “Big Shovels”
  - Packet Queue
- Packet Wrapping
  - Payload Encryption
  - Convert to Proto 99
  - TCP/UDP signal bit
- Targeting
  - key to network relationship

Key Management

- Multi-Key management is a joy
- Suggested Protections
  - Encrypt keys for the destination device
  - Never transmit in plaintext
  - Use alternate channels if possible
- Separated communications channel
  - SD Card/IR

Using the PropLANE

Badge Assembly



The Basics

- How to enroll your friends
  - Key.txt
- Protections the PropLANE provides
  - Encrypts communications on the blackside
- What the PropLANE won’t do
  - Fancy shit
- What you shouldn’t use the PropLANE for
  - Hiding from the Government
  - Banking
  - The lulz

Danger Will Robinson

- Crypto Implementation
  - Key size limitation
  - Speed
  - Single Key per device
    - It does not have to stay this way
- Expected privacy
  - If the key is not compromised, you're doing pretty good
- Difficulty in creating the PropLANE
  - Lots of beer, long nights, and pain

Future Goals

- Where we’d like to take the project
  - Try new algorithms (SIMON, SPECK, EU)
  - Complete a ARM port
  - Any direction you want
- What we think we can do in the future
  - Make crypto a feature on future electronic DC badges
  - Help protect the community and give people something to hack on

Administratum

- Where can I get the software and instructions?
  - https://github.com/proplane/proplane
- Where can I find more information?
  - http://www.proplane.org
- Contact info
  - firstname@proplane.org
- Drink Preference
  - Any

Questions?