Bastille

MATT KNIGHT // BASTILLE NETWORKS

GR-LORA

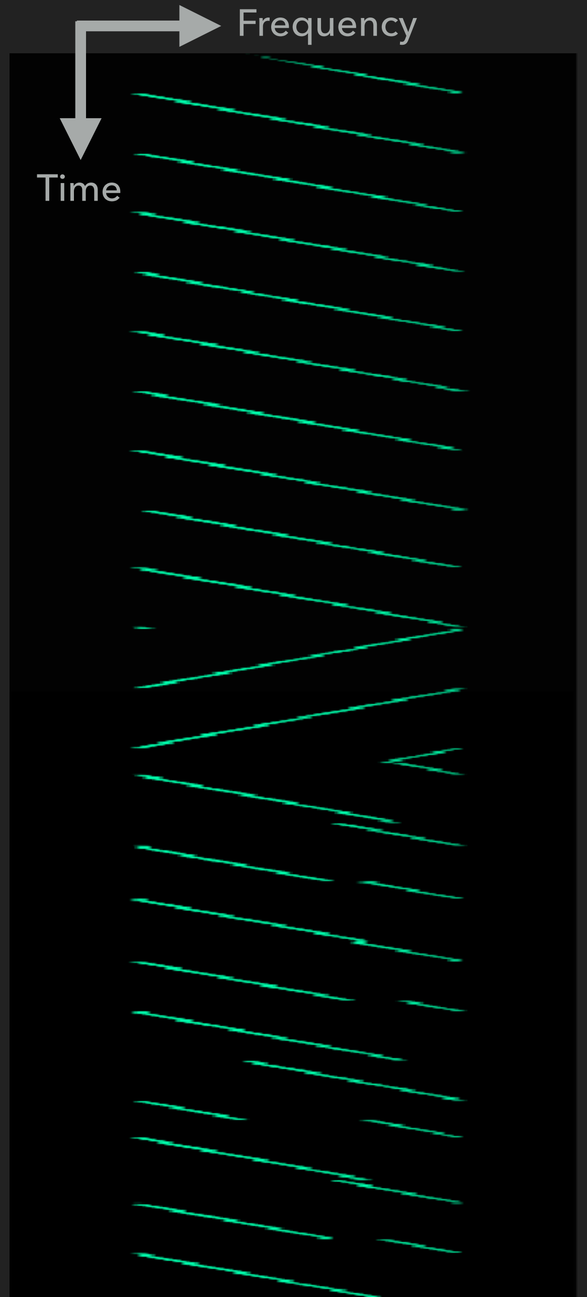
WHO'S THIS GUY

- Matt Knight
- Software Engineer and Threat Researcher @ Bastille
- BE & BA from Dartmouth
- Background in electrical engineering, embedded software, etc.
- Applied RF security research

matt@Bastille.net
@embeddedsec

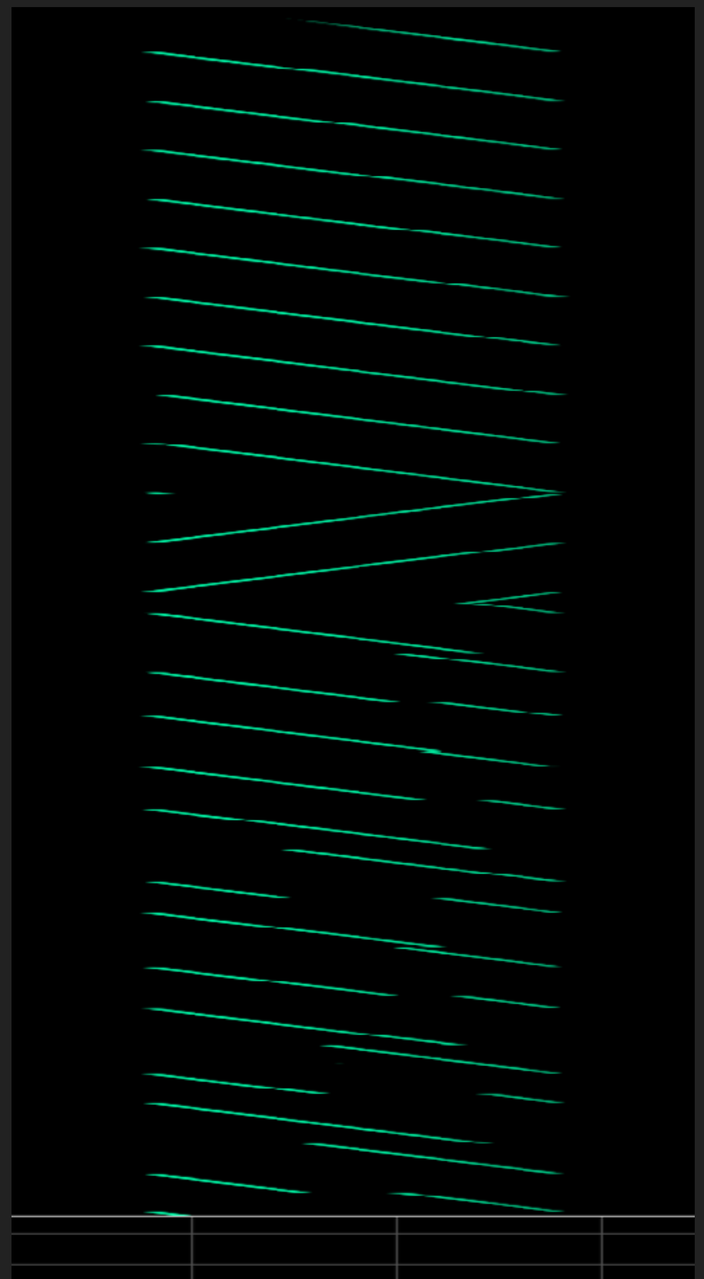
LORA

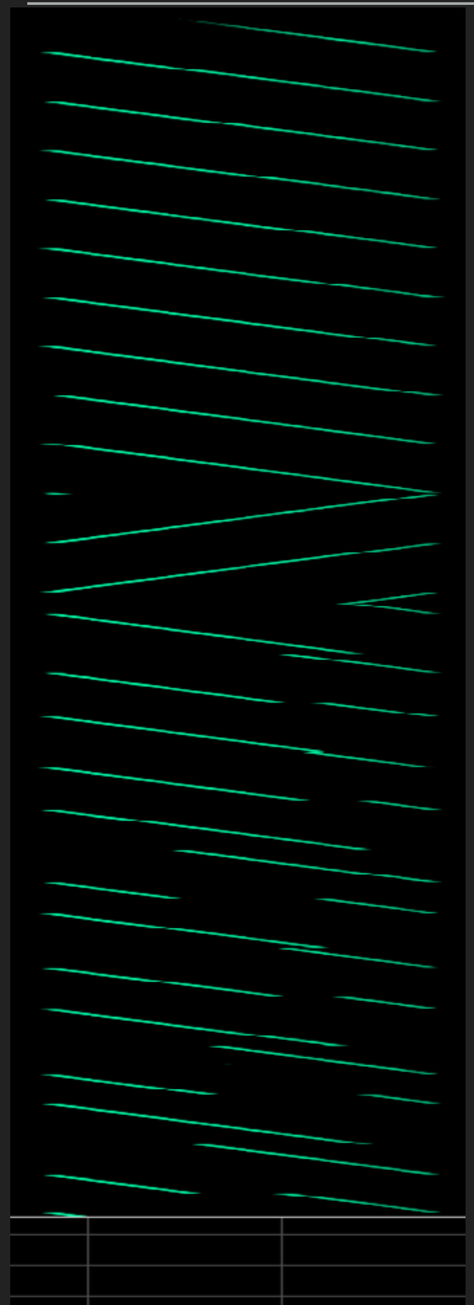
- “Long Range” wireless networking protocol
  - Optimized for embedded and IoT applications
  - Deployed in cellular topologies
- Chirp Spread Spectrum (CSS) modulation
  - Borrows RF features from RADAR systems
  - Long range + power efficiency at the expense of throughput



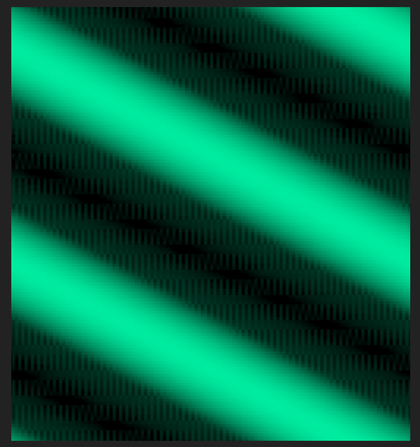
BLIND SIGNAL ANALYSIS PT. 1

- Modulation
  - Frequency modulated chirps
  - Each full chirp is a symbol, value determined by offset from preamble
- Demodulation process
  - De-chirp
  - N-bin wide FFT





*

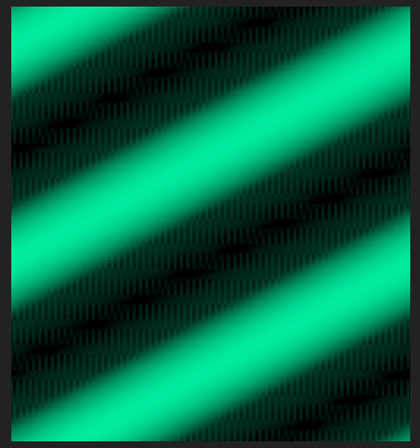


Upchirp

=

??

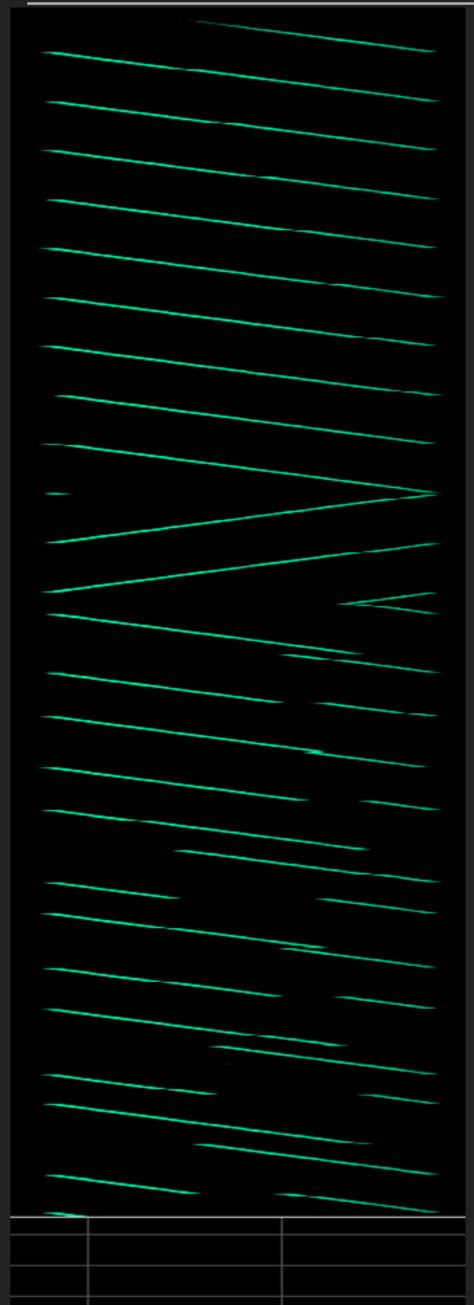
*



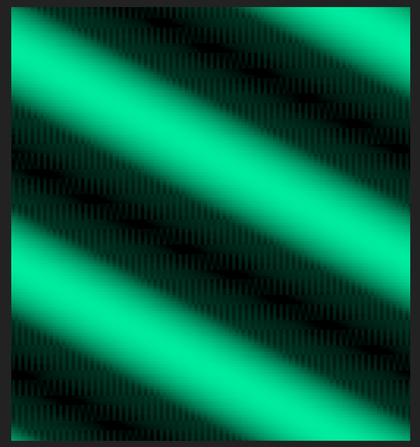
Downchirp

=

??

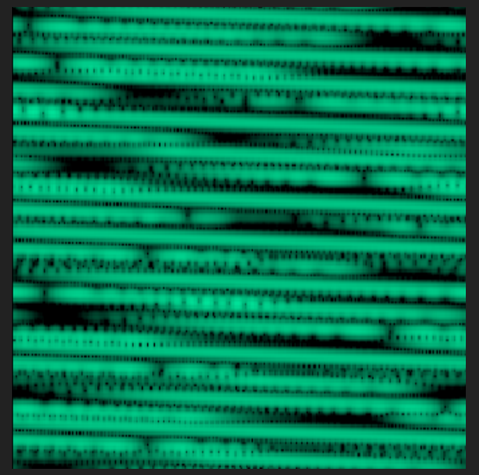


*



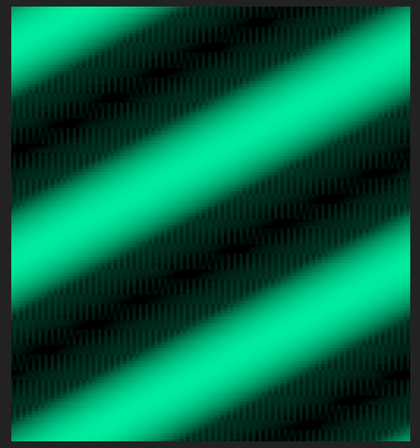
Upchirp

=



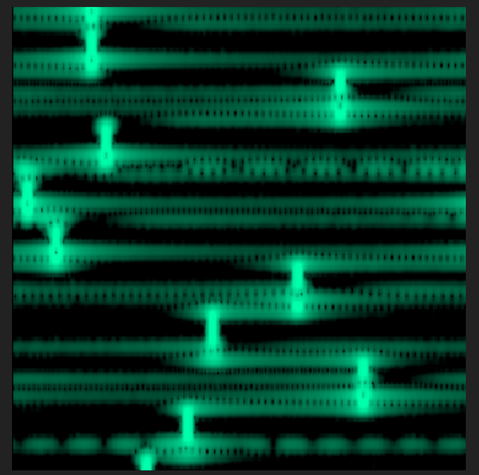
More spread

*

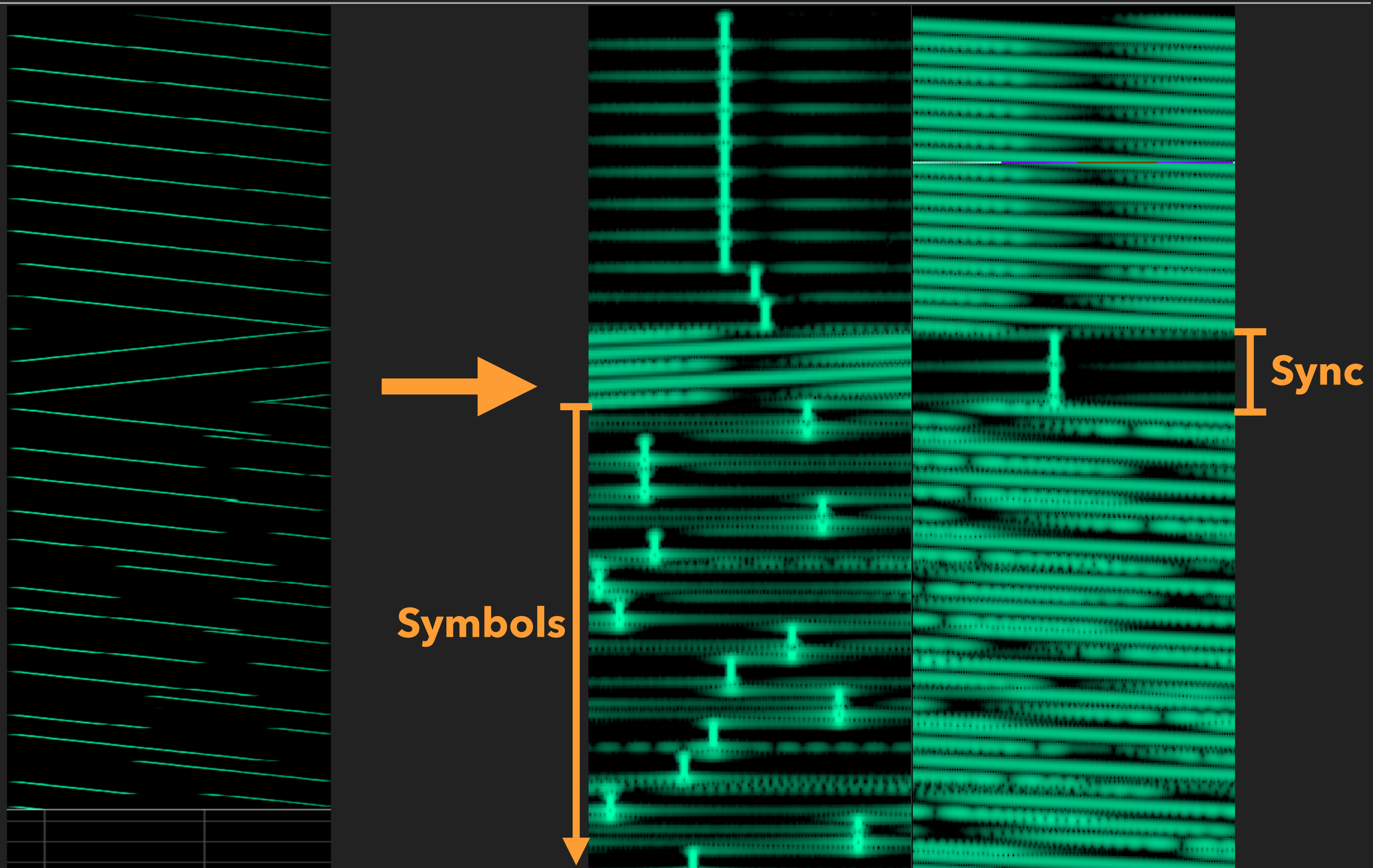


Downchirp

=



More friendly!


Symbols
Sync

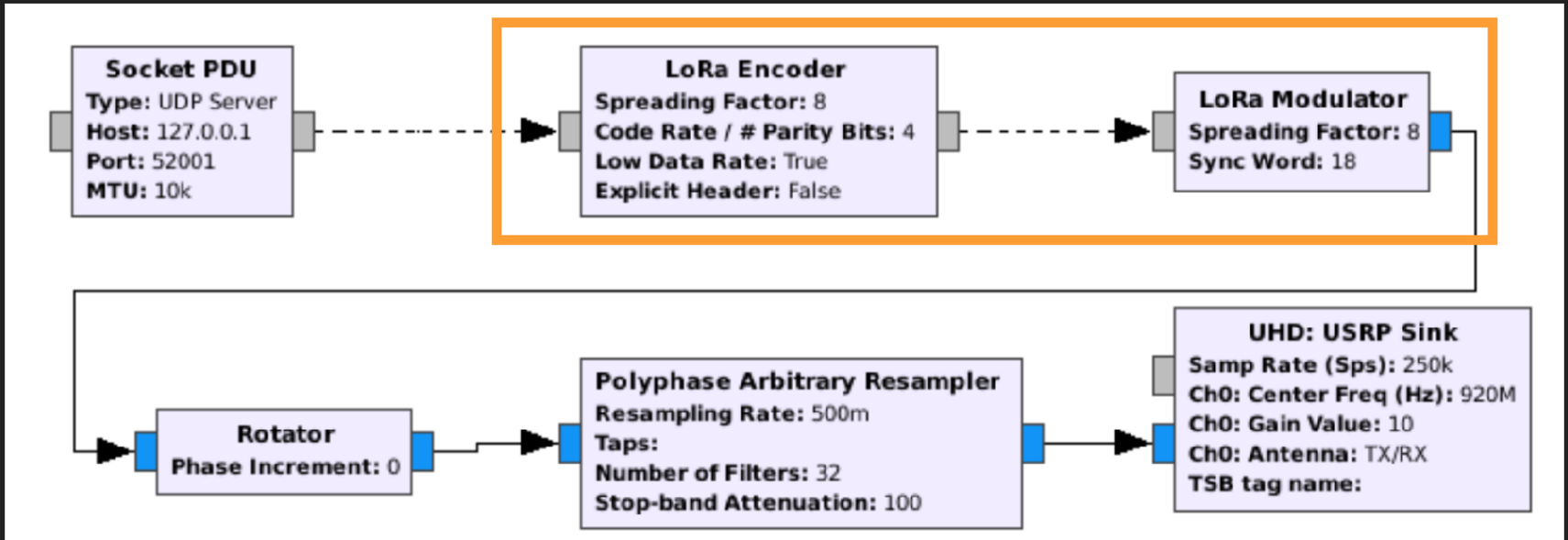
BLIND SIGNAL ANALYSIS PT. 2

- Encoding: multi-stage pipeline including
  - Reverse gray coding → Symbol off by +/-1 error tolerance
  - Whitening → Induces randomness for clock recovery
  - Interleaving → Spreads chips throughout PHY packet
  - Hamming FEC → Error recovery (parity bits on steroids)

- Research presented at 33c3, DEF CON Wireless Village, and Jailbreak Security Summit

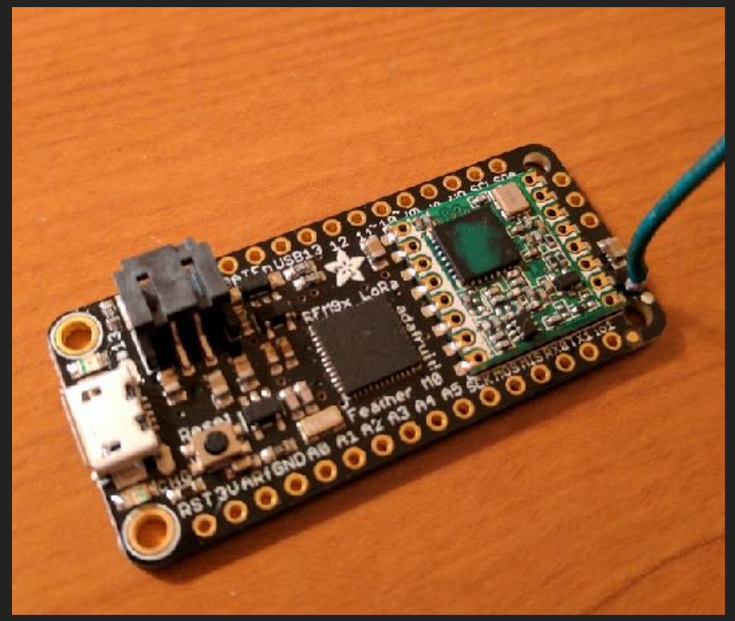
SDR AND GR-LORA

- Software Defined Radio
  - Protocol-specific features implemented in software rather than silicon
  - Rapid radio prototyping, reversing
- gr-lora
  - “Out of Tree” module for GNU Radio digital signal processing framework
  - Why? PHY layer security matters!



DEMO

- Transmitter
  - Semtech SX1272 hardware LoRa radio
  - Adafruit Arduino-like module



- Receiver
  - Ettus Research B210 Software Defined Radio
  - Demodulation by gr-lora

REFERENCES

Bastille

- Source Code
  - https://github.com/BastilleResearch/gr-lora.git
- 33c3 “Decoding LoRa” Talk
  - https://media.ccc.de/v/33c3-7945-decoding_the_lora_phy
- To learn more about wireless exploitation and PHY security:
  - “Radio Exploitation 101” at DEF CON 25, 1600 on Friday