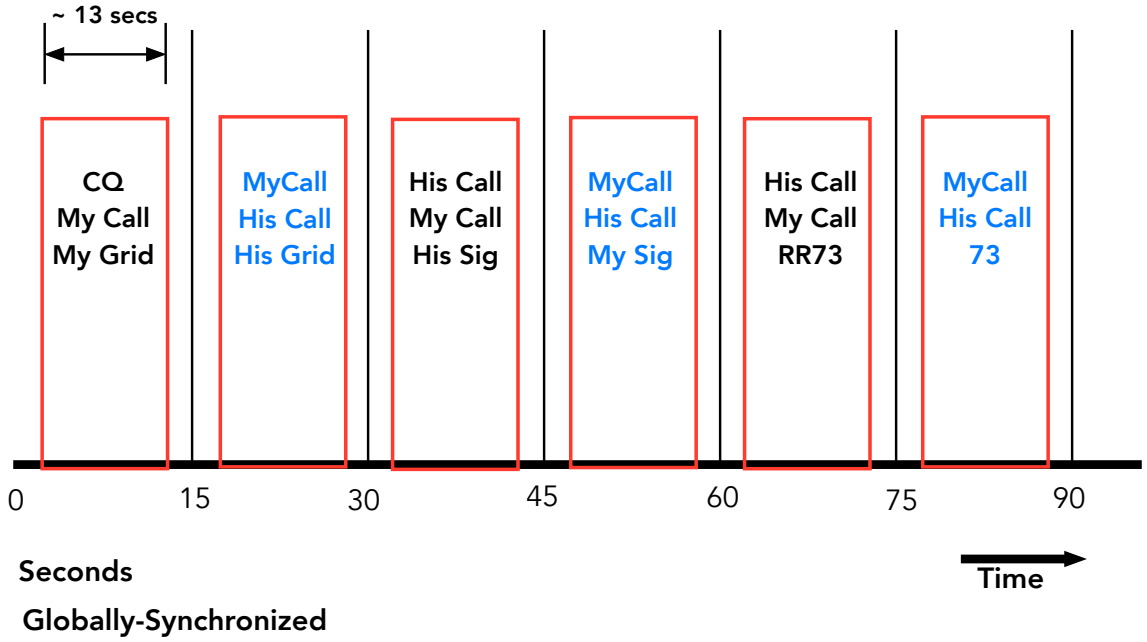
FT8 SuperFox

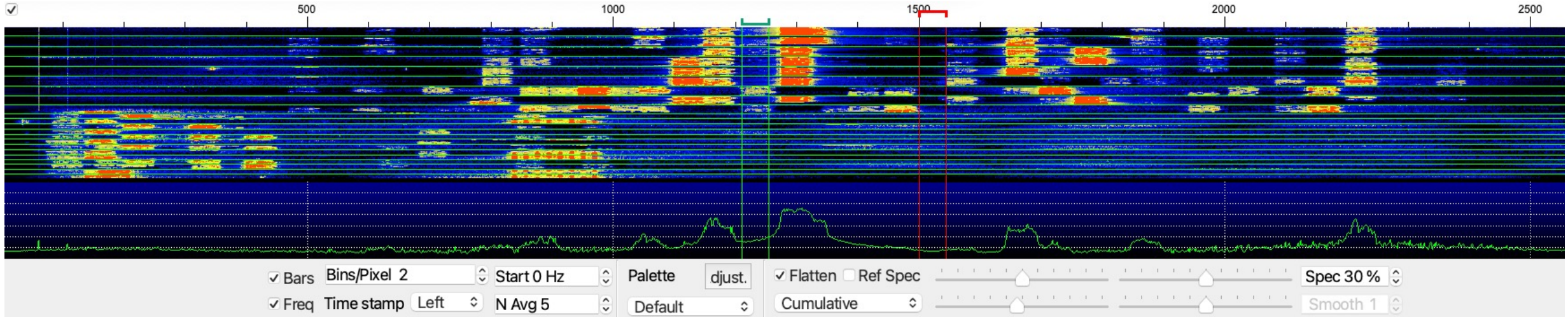
Typical FT8 Full Sequence

- Gaussian FSK (GFSK)

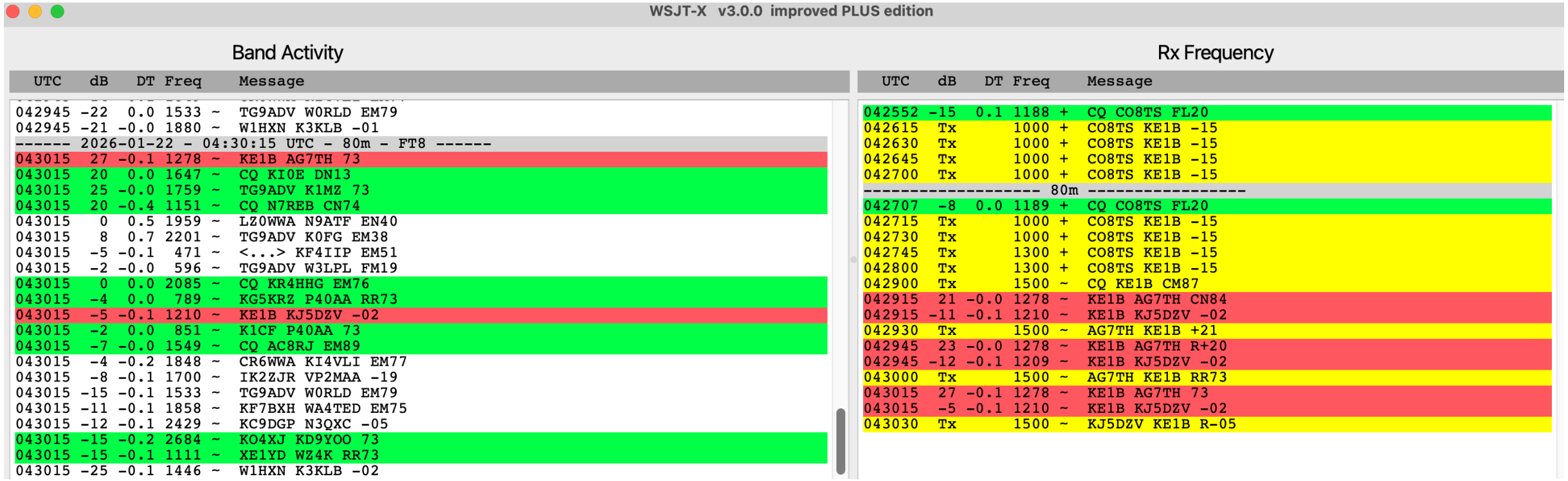
- 3 bits per symbol
- 2^3 = 8 discrete tones per symbol
- Globally-Synchronized Clocks
  All Transmissions on 15-second increments
- ~ 1 second “dead time” around transmission to allow for clock error
- Signal occupies 50 Hz of audio spectrum



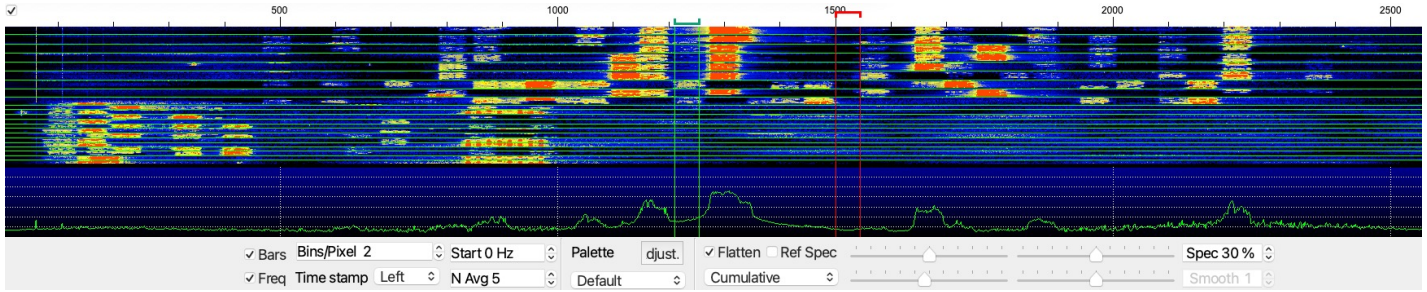
Typical FT8 Spectrum



Typical FT8 Exchange Sequence



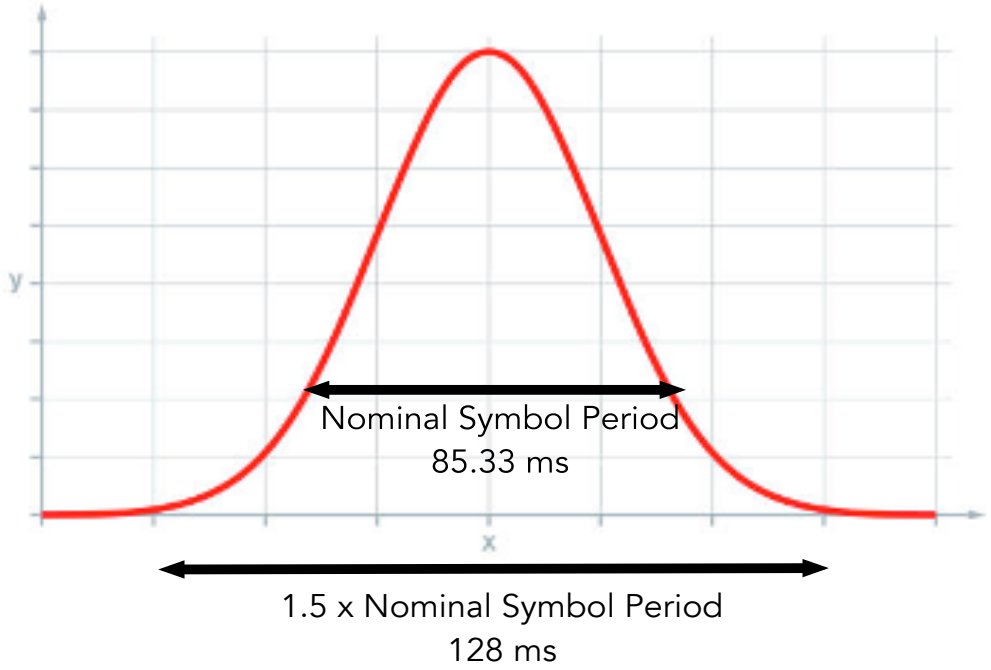
FT8 SuperFox



- Assumes only ONE “Fox” (DXpedition) and many ”Hounds” in the assigned audio spectrum
  Unlike ordinary FT8 where there can be many simultaneous callers and responders
- Take advantage of the fact that the Fox can use the entire audio spectrum for his transmissions
- Hounds still use ordinary FT8, 50 Hz per signal, so many Hounds fit in the audio spectrum
- Fox uses 1500 Hz of spectrum, nominally 750 – 2250 Hz
- Can support up to NINE simultaneous Hounds in QSO with the single Fox
- Still requires Globally-Synchronized Clocks
  All Transmissions still on 15-second increments
- ~ 1 second “dead time” around transmission to allow for clock error

SuperFox Symbol Transmission Characteristics

- Gaussian FSK (GFSK)
- 7 bits per symbol
- 2^7 = 128 discrete tones per symbol
- Base frequency = 750 Hz
- Tones spaced 11.71875 Hz apart (baud rate)
  85.33 ms per symbol
- Bandwidth used = 128*11.71875 = 1500 Hz
  Frequency range = 750 to 2250 Hz



SuperFox Message Structure

350 bits per message

50 symbols @ 7 bits per symbol
(plus synchronization and error correction)

Last 3 symbols (21 bits) are always checksum (nhash2 function)

329 bits available for message payload

Three Message Types:
- Type 0: Standard (Signal Reports + RR73)
- Type 2: Free Text + 4 Hounds
- Type 3: CQ + Grid + Free Text

Standard Message

- All callsigns hashed to fit into 28 bits, if needed
- Only callsigns ≤ 5 chars can be encoded in 28 bits (base 38 encoding: A-Z, 0-9, /, space)

Fox Call	28 bits
Hound Call 1 (implicit RR73)	28 bits
Hound Call 2 (implicit RR73)	28 bits
Hound Call 3 (implicit RR73)	28 bits
Hound Call 4 (implicit RR73)	28 bits
Hound Call 5 (implicit RR73)	28 bits
Hound Call 6	28 bits
Hound Call 7	28 bits
Hound Call 8	28 bits
Hound Call 9	28 bits
Sig Report 6	5 bits
Sig Report 7	5 bits
Sig Report 8	5 bits
Sig Report 9	5 bits
(reserved)	5 bits
mCQ	1 bit
Message Authentication Code (OTP)	20 bits
Msg Type = 0	3 bits
	329 bits total

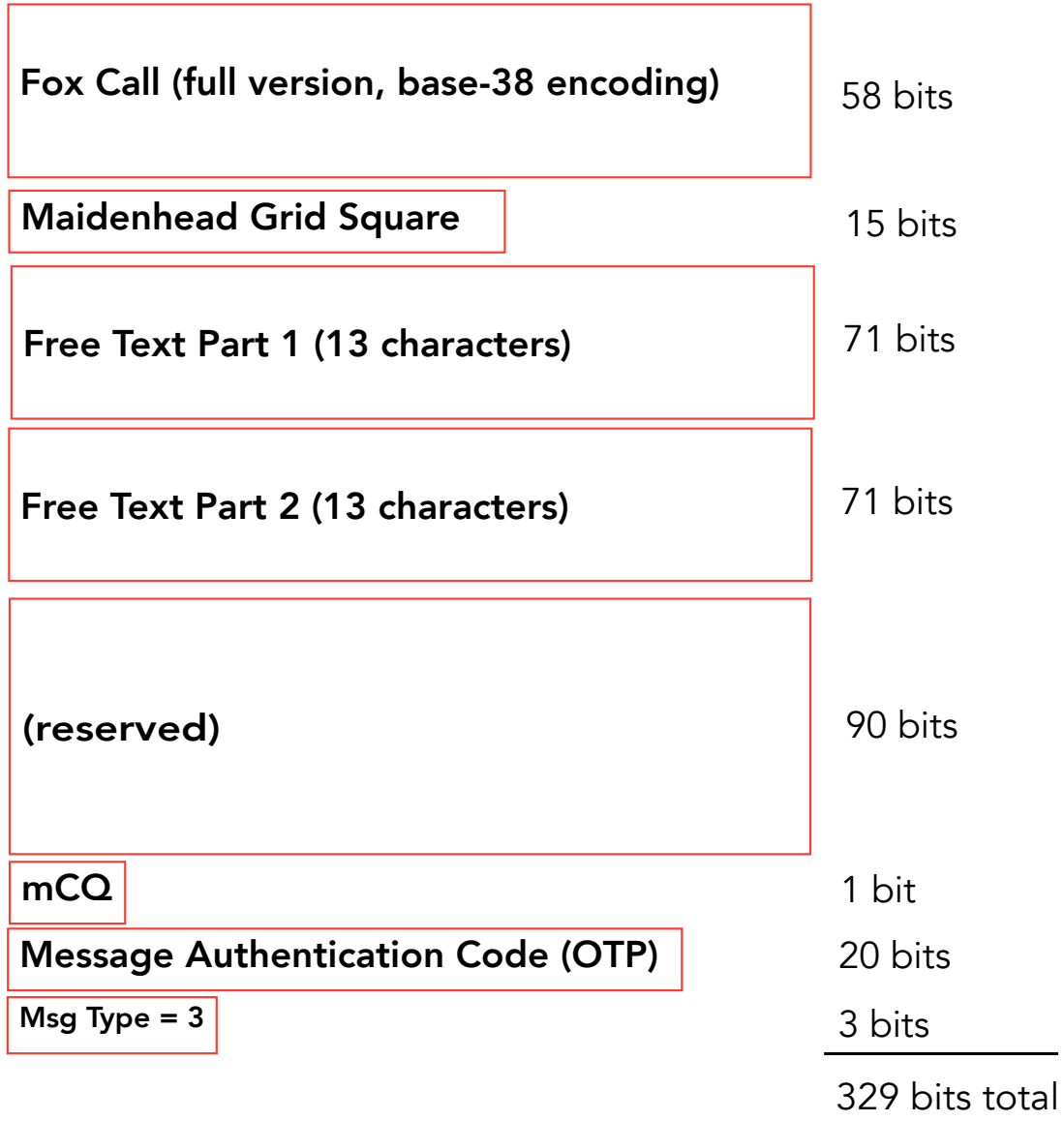
Free Text Message

- All callsigns hashed to fit into 28 bits, if needed
- Only callsigns ≤ 5 chars can be encoded in 28 bits (base 38 encoding: A-Z, 0-9, /, space)

Fox Call	28 bits
Hound Call 1	28 bits
Hound Call 2	28 bits
Hound Call 3	28 bits
Hound Call 4	28 bits
Sig Report 1	5 bits
Sig Report 2	5 bits
Sig Report 3	5 bits
Sig Report 4	5 bits
Free Text Part 1 (13 characters)	71 bits
Free Text Part 2 (13 characters)	71 bits
(reserved)	3 bits
mCQ	1 bit
Message Authentication Code (OTP)	20 bits
Msg Type = 2	3 bits
	329 bits total

CQ + Grid + Free Text Message

- Typically sent once every few minutes
- Fox callsigns up to 11 characters can be sent without hash/loss of information in 58 bits
- Base-38 encoding: A-Z, 0-9, space, /
- 38 ^ 11 ≈ 2.4 x 10^17; 2^58 ≈ 2.9 x 10^17
  Any reasonable callsign fits in code space



Report Encoding

5 bits (can encode values from 0 – 31)

Signal report is range between -18 to +12
Encode as (n + 18)

Value of 31 (all ones) interpreted as “RR73”

Free Text Encoding

Custom 71 bit code

Character Set (42 possible values):
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_+-./?’

13 characters per block:
42^13 ≈ 1.3 x 10^21 encodes into space of 71 bits: 2^71 ≈ 2.4 x 10^21

Message Authentication

- This crazy guy* issues a secret 16-character code, e.g.:

  5DF6 KZ6Q RMNG GW2X

- Characters chosen from: A-Z, 2-7
  32 possible characters, 5 bits/character, 80 bits total
- Every SuperFox station gets a different secret code
- Secret code is privately communicated to DXpedition leader, and also loaded onto SuperFox Authentication Server: www.9dx.cc

* The Northern CA DX Foundation is the official distributing organization for SuperFox keys. Rich KE1B is the current NCDXF SuperFox key administrator.

SuperFox Station Generates Sequence of “One Time Passwords” (OTPs) in Real Time

- 80 bits of secret code (2^80 ≈ 1.2 x 10^24)
- Timestamp: FLOOR (unix_seconds ÷ 30)

  unix_seconds = # of seconds since 1 January 1970
  Current values are ~ 1.7 billion

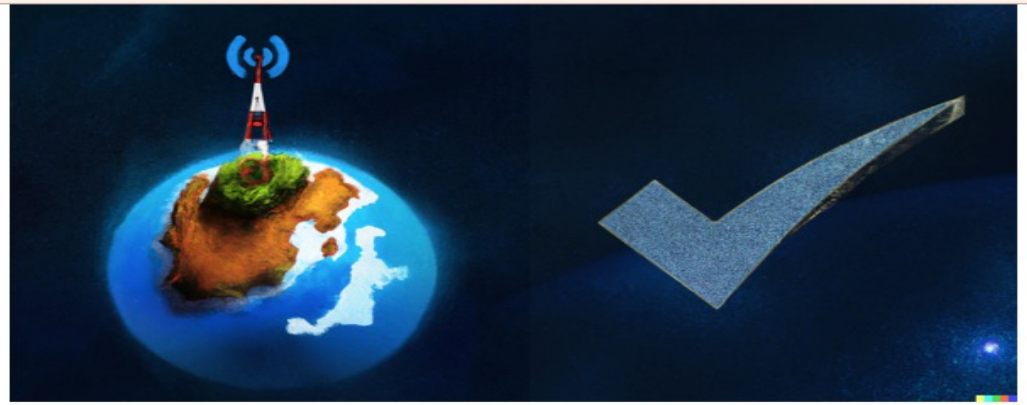
  All SuperFox transmissions are on globally-synchronized 30-second windows
- Compute HMAC-SHA1 (secret code, timestamp)
  Output is 160 bit cryptographic hash function
  Truncate to 31 bits using RFC 4226 algorithm (select bits)
- Divide result by 1,000,000 to generate a number between 0 – 999,999 (One Time Password)
- Transmit OTP in every Fox message, 20 bits of payload (2^20 ≈ 1 million)

Hounds Authenticate via Internet

- Authentication server at www.9dx.cc computes OTP for every possible timestamp and every active SuperFox station
- New value every 30 seconds per station, # between 0 – 999,999
- User software sends Fox callsign, timestamp and received OTP to server
- Instant authentication and verification; User gets “VERIFIED” message as part of display in WSJT-X software (software accesses server in real-time during QSO)
- Timestamp can be +/- one 30-second interval to allow for time variation
- Can also query server at any time after QSO to validate OTP (useful if Hound does not have Internet access during QSO)

www.9dx.cc Home Page

www.9dx.cc



Is it really them?

How do you know that Fox is the real DX? If they're transmitting a verification code, use this website to see if their codes matches what they should be.

Enter the DX callsign to get started:

Submit Query

Example query

Last five minutes of verification codes for V6CU25.

Callsign	Date	Timestamp	Code
V6CU25	20260116	220700	062936
V6CU25	20260116	220730	029368
V6CU25	20260116	220800	395256
V6CU25	20260116	220830	530708
V6CU25	20260116	220900	923826
V6CU25	20260116	220930	013249
V6CU25	20260116	221000	678659
V6CU25	20260116	221030	137998
V6CU25	20260116	221100	355591
V6CU25	20260116	221130	002089
V6CU25	20260116	221200	932089

Make sure that the Code and the Timestamp **BOTH** match what was sent by the station claiming to be V6CU25.

Difficult for Pirate Station to Pretend to be real DXpedition

- 80 bit secret key is much too large for brute force attack
- Use of timestamp in generation of OTP prevents “playback” imitation
- IN THEORY, Pirate could implement his own authentication server (which would incorrectly verify the pirate as the real McCoy), BUT:
- www.9dx.cc Authentication Server is default/burned into WSJT-X
- Pirate would need to change that setting in EVERY Hound station
- Current authentication scheme has never been hacked/broken

Ordinary FT8 vs. SuperFox

Characteristic	FT8	SuperFox
Transmit Bandwidth	50 Hz	1500 Hz
Max QSO rate	~50-100 QSOs/hour	~350-400 QSOs/hour
Authentication	No	Yes
Free Text Capability	No	Yes
Hounds per transmission	1 per stream	Up to 9 in one stream
Modulation	8-GFSK	128-GFSK
Transmit Time	12.64 secs	12.88 secs