True Random Number Generation from Very Low Frequency Noise

Matei Barbu

Dumitru-Cristian Trancă

Florin-Alexandru Stancu

github.com/mateibarbu19/trng-methods

RoEduNet 2025

Why?

> Cryptographic system should remain secure even if all details about the system, except for the secret key, are publicly known. – Kerckhoffs' principle

Why?

> Cryptographic system should remain secure even if all details about the system, except for the secret key, are publicly known. – Kerckhoffs' principle

So, how do we choose a secret?

RANDOM.ORG [Haa25]

Figure 1: Version 1
(with whiskey bottles)

Figure 2: Version 2

Related Work

- A embedded prototyping approach [LL19]
  - Focused on maximizing entropy
  - Non i.i.d. variables
  - Comparison between compressed and uncompressed streams
  - Plots use are misleading
  - Leaked audio noise at acquisition
  - Good results when combining multiple sources

Related Work

- A embedded prototyping approach [LL19]
  - Focused on maximizing entropy
  - Non i.i.d. variables
  - Comparison between compressed and uncompressed streams
  - Plots use are misleading
  - Leaked audio noise at acquisition
  - Good results when combining multiple sources
- A on-chip 180nm approach [Kum+20]
  - Employed hybrid sources of entropy
    - QRNG based on optical phenomena
    - Un compressed radio captures
  - They propose an unconventional arbiter block
  - Important implementation details were left out

Research Objectives

- Reproducible results
- Modular design
- FIPS 140-2 validation

Very Low Frequency Radio

- 3-30kHz
- Ideally in a Radio Quiet Zone
- Data from **abelian.org**

> The atmospheric noise in VLF band is mainly impulse noise under the background of Gaussian white noise. Gaussian white noise is composed of the superposition of pulses formed by a large number of thunderstorms distributed around the world. Impulse noise is formed by the superposition of lightning electromagnetic pulses near the receiver. [LXC22]

Figure 3: Setting up an antenna in Alaska [Stu25]

VLF Characteristics I

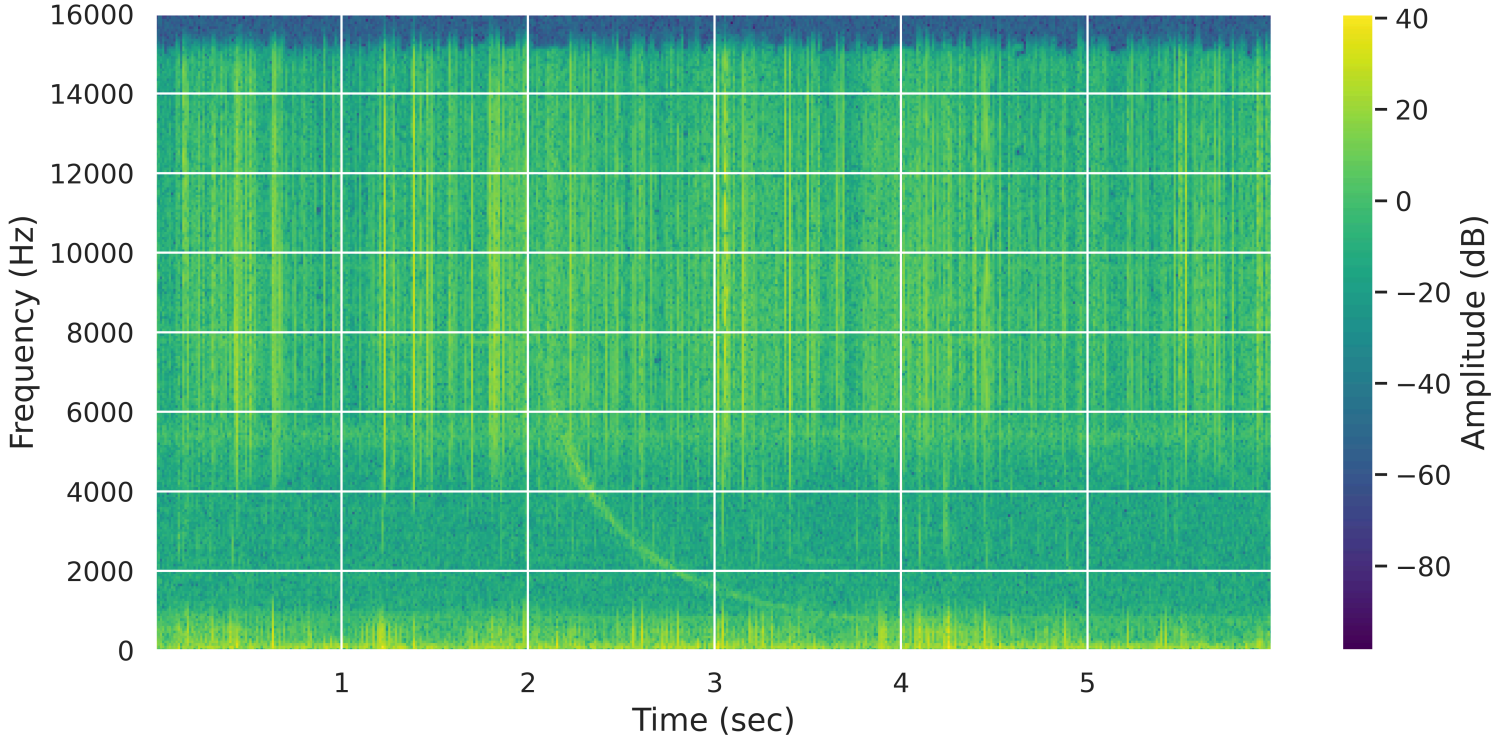


Figure 4: General spectrogram pattern for VLF captures. Whistler portrayed in the center bottom. Lightning events depicted by vertical yellow bars.

VLF Characteristics II

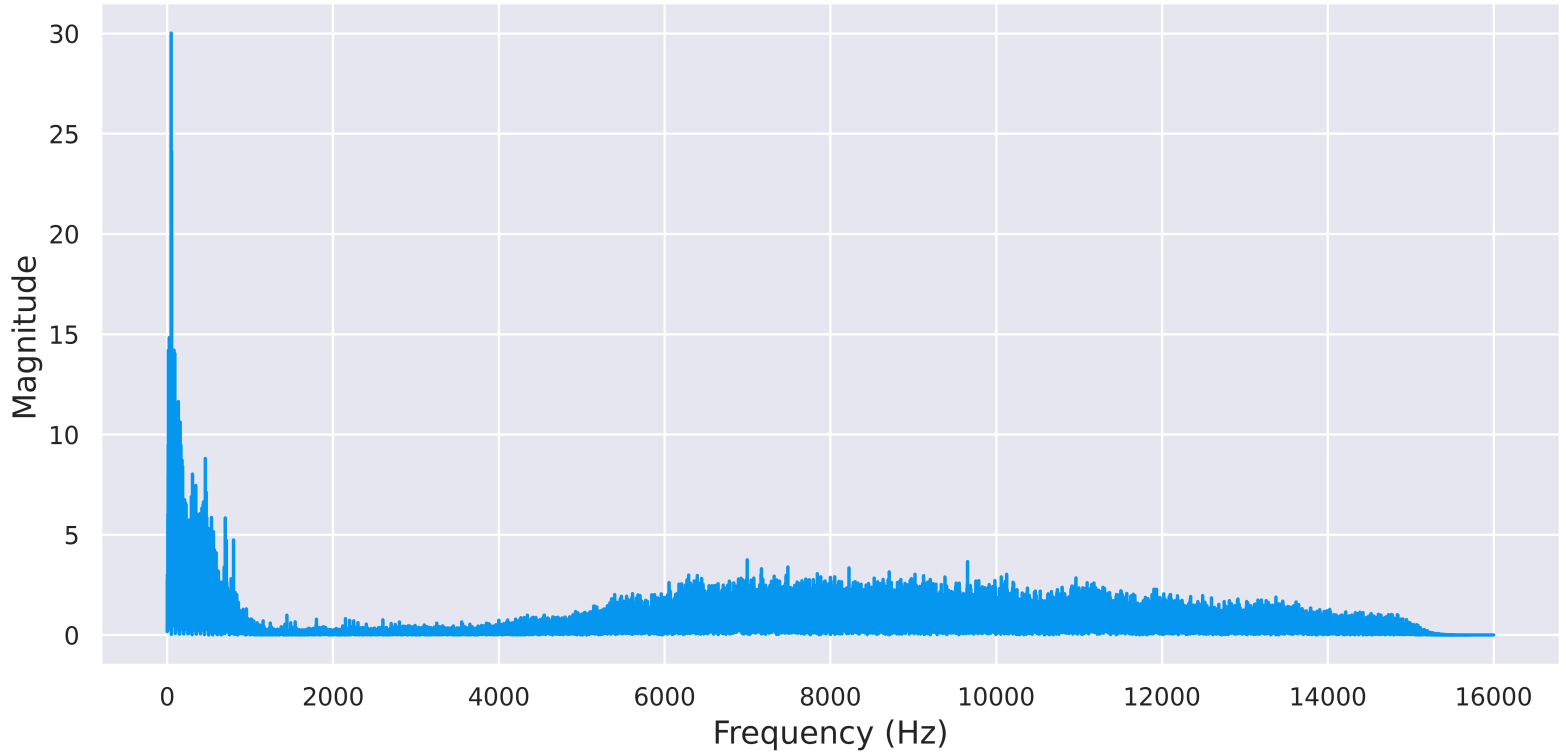


Figure 5: General spectrum pattern for VLF captures.

VLF Characteristics III

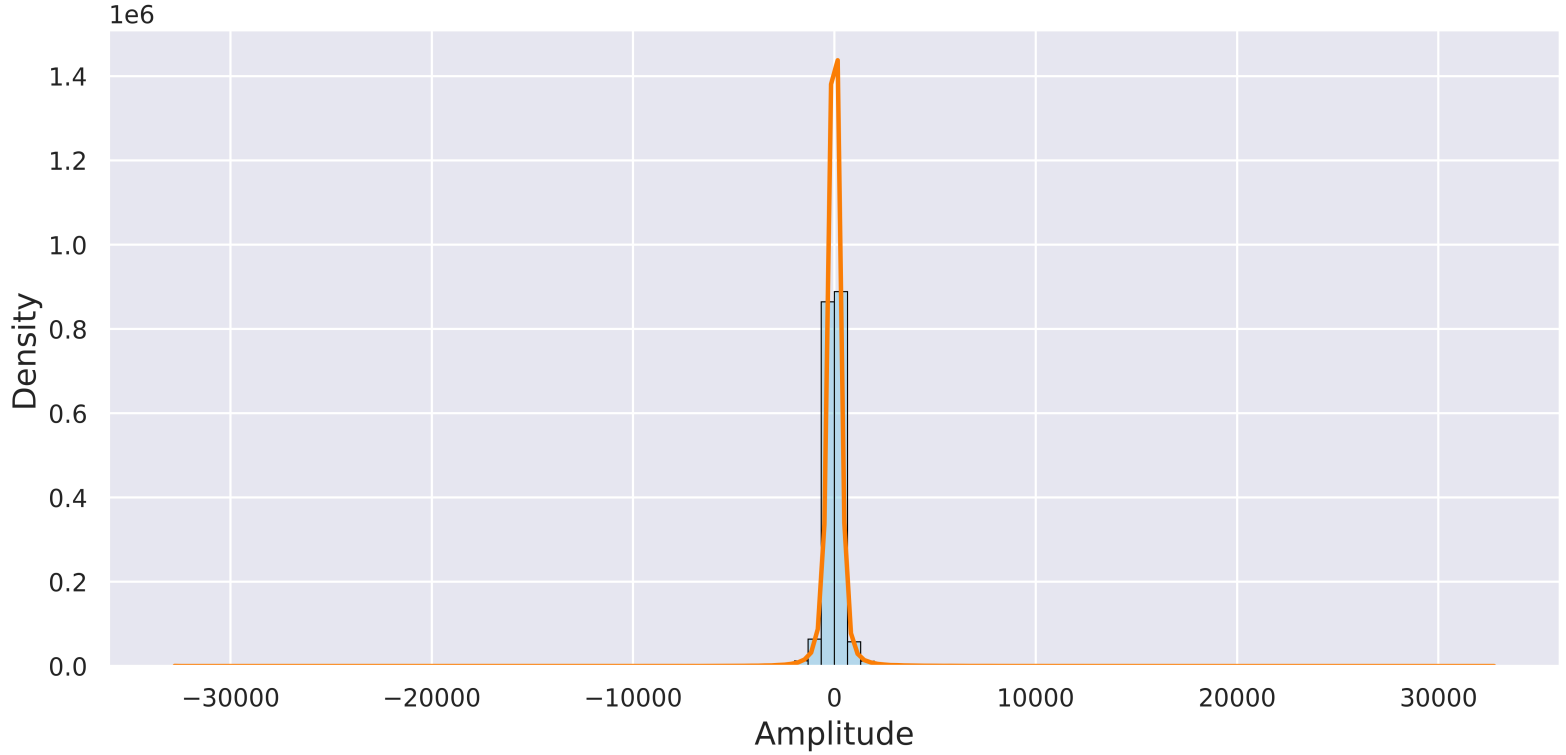


Figure 6: General distribution pattern for VLF captures.

Our Proposal

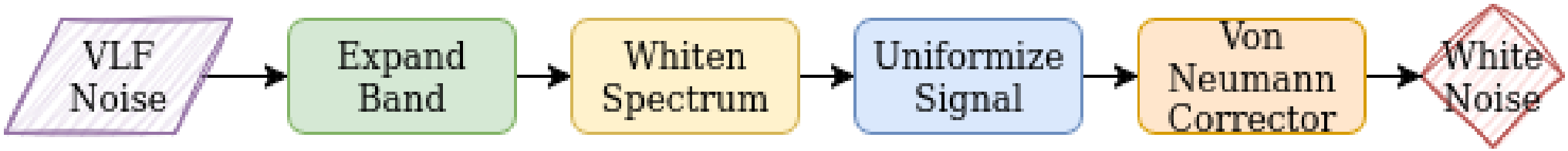


Figure 7: Post-processing pipeline for a VLF entropy source

Our Proposal

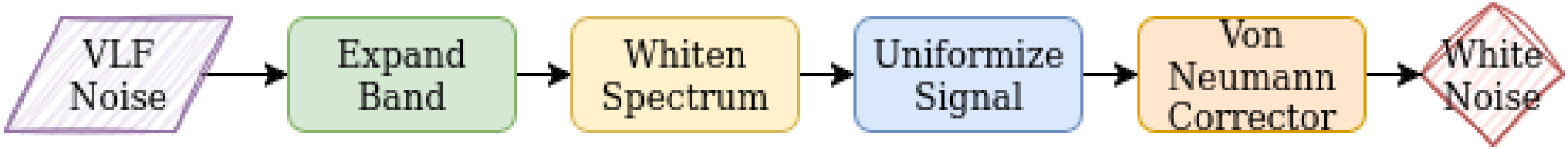


Figure 7: Post-processing pipeline for a VLF entropy source

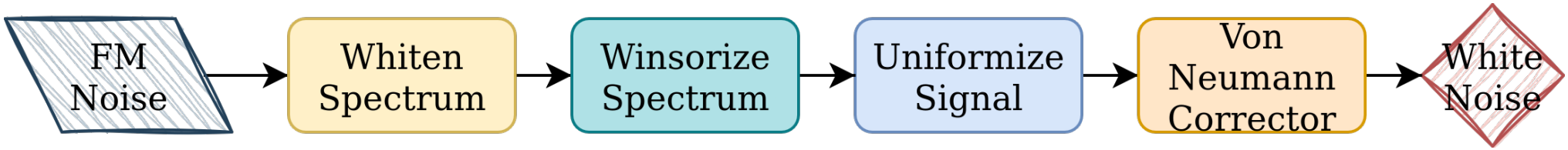


Figure 8: Post-processing pipeline for a FM entropy source

Experiments

Host Id	Location	Coordinate
15	Cumiana, NW Italy	44.96N,7.42E
35	Forest, Virginia	37.34385N,79.28818W
41	Heidelberg, Germany	49.443N,8.695E

Table 1: Chosen VLF hosts from abelian.org

Experiments

Host Id	Location	Coordinate
15	Cumiana, NW Italy	44.96N,7.42E
35	Forest, Virginia	37.34385N,79.28818W
41	Heidelberg, Germany	49.443N,8.695E

Table 1: Chosen VLF hosts from abelian.org

Host Id	Entropy (b/B)	Optimum compression reduction (%)	Arithmetic mean	Monte Carlo Pi error (%)	Serial correlation coefficient
15	6.151641	23	126.6439	30.24	0.124103
35	4.797632	40	126.6439	14.82	0.493773
41	6.708163	16	127.6324	27.95	0.026920

Note. Chi squared percentage of 0.01% on all sources.

Table 2: Evaluation of VLF entropy sources distributions

Results

High entropy (~8b/B), unbiased, low correlated outputs.
On average, the VLF pipeline failed about 300-400 tests out of ~425000, resulting in an 0.0008 error rate. Which is comparable to the $p = 0.001$ threshold within the SP800 STS suite.

Results

High entropy (~8b/B), unbiased, low correlated outputs.
On average, the VLF pipeline failed about 300-400 tests out of ~425000, resulting in an 0.0008 error rate. Which is comparable to the $p = 0.001$ threshold within the SP800 STS suite.

Host Id	Passed	Failed	Weak	Percentage
15	100	11	3	87%
35	101	10	3	88%
41	92	12	10	80%

Table 3: Dieharder results for our TRNG pipeline on VLF sources

Comments

- Von Neumann corrector is the “weak link” in the chain
  - output bitrate $\approx 25\%$ input bit rate
  - too generic
  - causes some `dieharder` tests to fail
- Noise up to 4kHz is discarded
- Multiple FFTs on blocks of different sizes

Further Improvements

- Optimize parameters
  - Data representation size
  - Sample rate
  - Block sizes
- Replace algorithms with more performative ones
  - E.g. Von Neumann corrector with a cryptographic hash function
  - Reduce operations on spectrum
- Dynamically determine the shape of the Gaussian white noise envelope

Further Improvements

- Optimize parameters
  - Data representation size
  - Sample rate
  - Block sizes
- Replace algorithms with more performative ones
  - E.g. Von Neumann corrector with a cryptographic hash function
  - Reduce operations on spectrum
- Dynamically determine the shape of the Gaussian white noise envelope
- Use higher quality VLF sources

Thank you for listening!

- Contact:
  - **matei.barbu1905@stud.acs.upb.ro**
  - dumitru.tranca@upb.ro
  - florin.stancu@upb.ro

github.com/mateibarbu19/trng-methods

> Randomness works well in search sometimes better than humans.
>
> – Nassim Nicholas Taleb

Bibliography

[Haa25] M. Haahr, “RANDOM.ORG: True Random Number Service.” Accessed: Jun. 28, 2025. [Online]. Available: https://random.org/

[LL19] K. Lee and M. Lee, “True random number generator (trng) utilizing fm radio signals for mobile and embedded devices in multi-access edge computing,” *Sensors*, vol. 19, no. 19, p. 4130, 2019.

[Kum+20] D. Kumar, C. D. Jadhav, P. K. Misra, and M. Goswami, “Opto-Radio Noise based True Random Number Generator,” in *2020 24th International Symposium on VLSI Design and Test (VDAT)*, 2020, pp. 1–5.

[LXC22] G. Li, J. Xie, and J. Chu, “Study on the characteristics of VLF atmospheric noise and its influence on the receiving performance,” in *2022 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 2022, pp. 1–5.

[Stu25] R. Sturtz, “Researchers preserve and release trove of public, low-frequency radio wave data.” Accessed: Sep. 16, 2025. [Online]. Available: https://news.ucdenver.edu/researchers-preserve-and-release-trove-of-public-low-frequency-radio-wave-data/

[Gu+22] X. Gu *et al.*, “First Results of the Wave Measurements by the WHU VLF Wave Detection System at the Chinese Great Wall Station in Antarctica,” *Journal of Geophysical Research: Space Physics*, vol. 127, p. , 2022, doi: 10.1029/2022JA030784.

FM as an Entropy Source

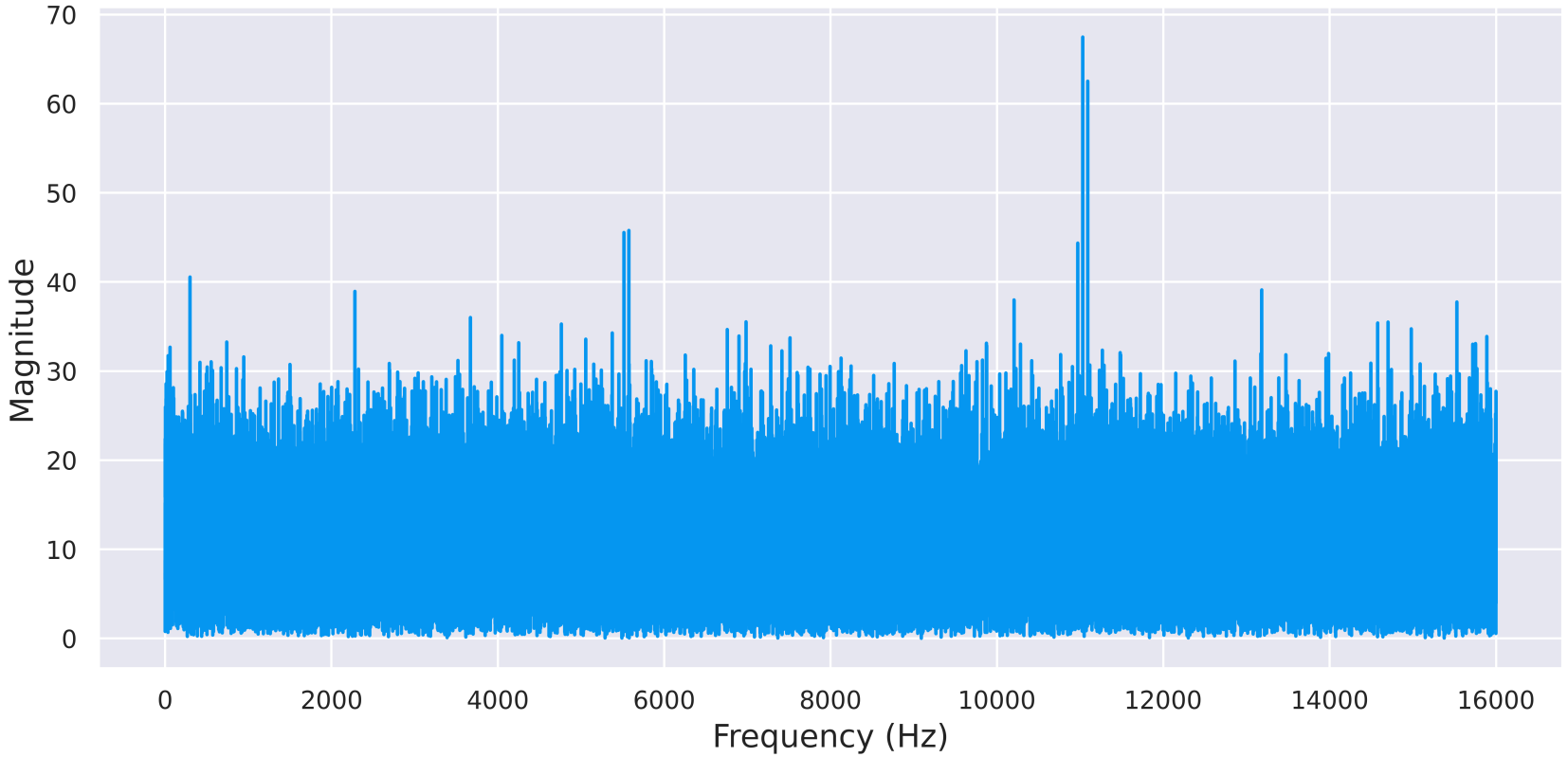


Figure 11: General spectrum pattern for an FM source

FM as an Entropy Source

Frequency (MHz)	Entropy (b/B)	Optimum compression reduction (%)	Arithmetic mean	Monte Carlo Pi error (%)	Serial correlation coefficient
80	7.300621	8	127.1270	21.81	0.015797
160	7.473322	6	129.8854	21.42	0.008358
230	7.343521	8	127.7567	21.70	0.013876

Note. Chi squared percentage of 0.01% on all sources.

Table 4: Evaluation of FM entropy sources distributions

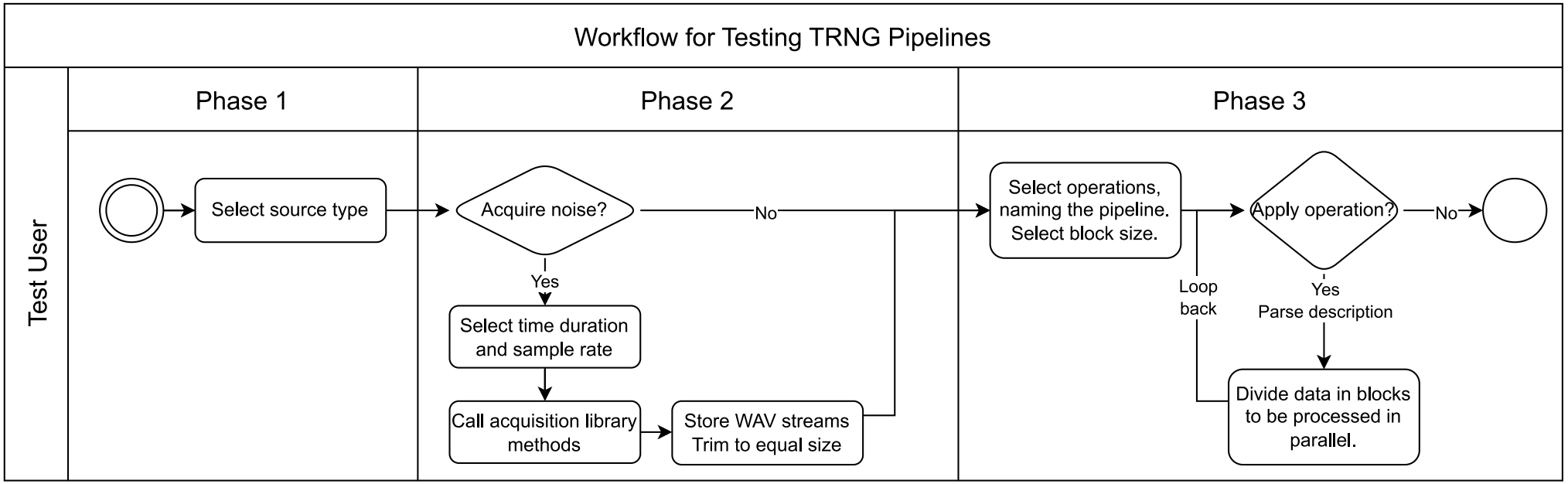
FM as an Entropy Source

Frequency (MHz)	Monobit	Poker	Runs	Long Run	Continuous run	Total
80	3	1	8	9	0	20
160	5	2	5	4	0	16
230	1	1	3	7	0	12

Note. Mesured with `rngtest`.

Table 5: Failed FIPS 140-2 tests out of 23024 for the FM pipeline

Software flow



Algorithms

Algorithm 1: Expand Band

1 spectrum ← FFT(data)
2 band_spectrum ← spectrum[start:end]
3 factor ← $\frac{\text{spectrum.size}}{\text{end}-\text{start}}$
4 spline_degree ← 5
5 enlarged_spectrum ← ZOOM(band_spectrum, factor, spline_degree)
6 adjusted_data ← IFFT(enlarged_spectrum)

Algorithms

Algorithm 2: Quantile Normalization For Uniform Distribution

1 max $\leftarrow$ MAXIMUM(ABS(data))
2 data $\leftarrow \frac{\text{data}}{\text{max}}$
3 ranked_data $\leftarrow$ RANK(data)
4 uniform_data $\leftarrow \frac{\text{ranked\_data}}{\text{ranked\_data.len}}$

More on VLF receivers [Gu+22]

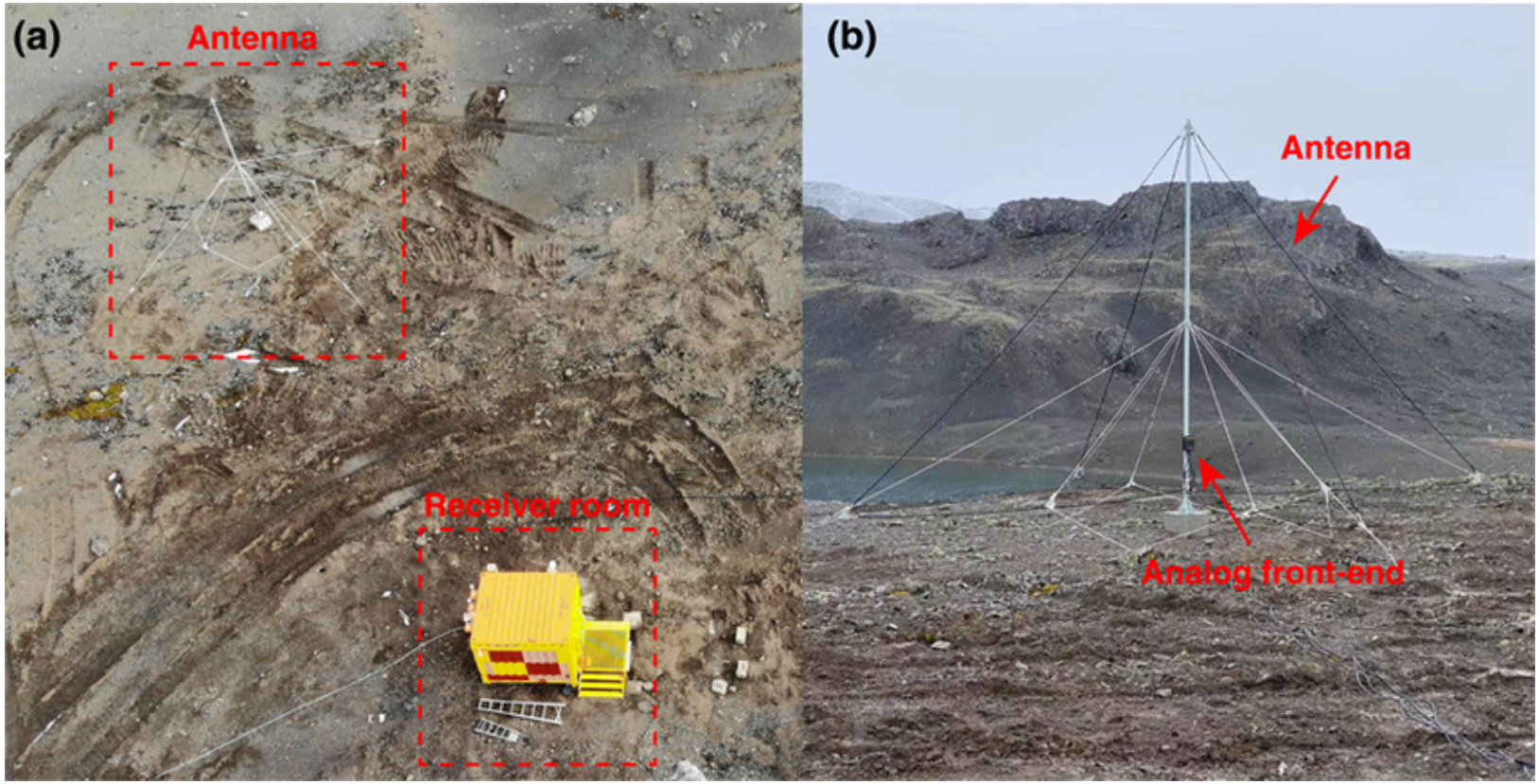


Figure 12: Photos of the Extremely Low Frequency/Very Low Frequency receiving system at the Great Wall station in Antarctica, (a) Layout and (b) antenna structure.