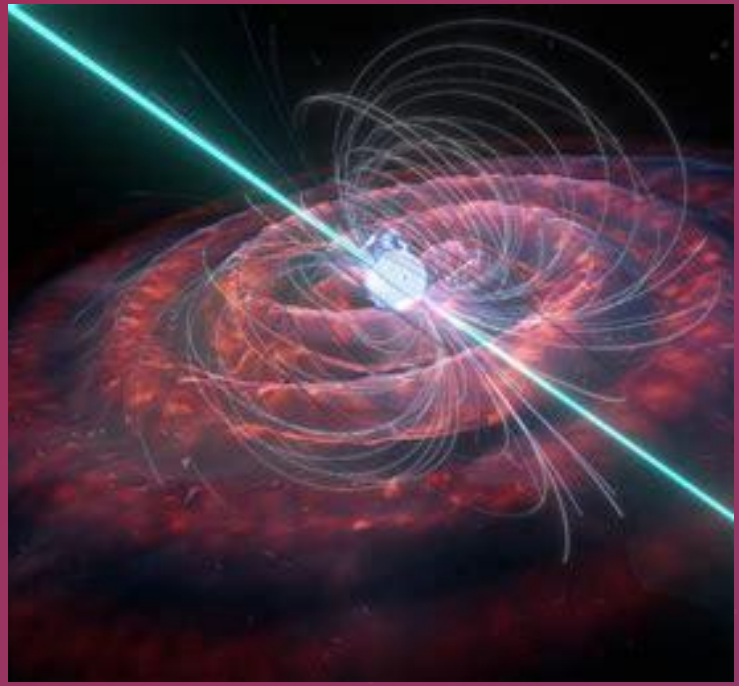
Pulsar Leakage Analysis

Emma Stensland

What Are Pulsars?

- Pulsars are electromagnetic signals generated on the magnetic poles of neutron stars.
- When neutron stars rotate, this signal passes over earth, and we detect them as periodic electromagnetic pulses.
- (A.K.A. Space Lighthouses)



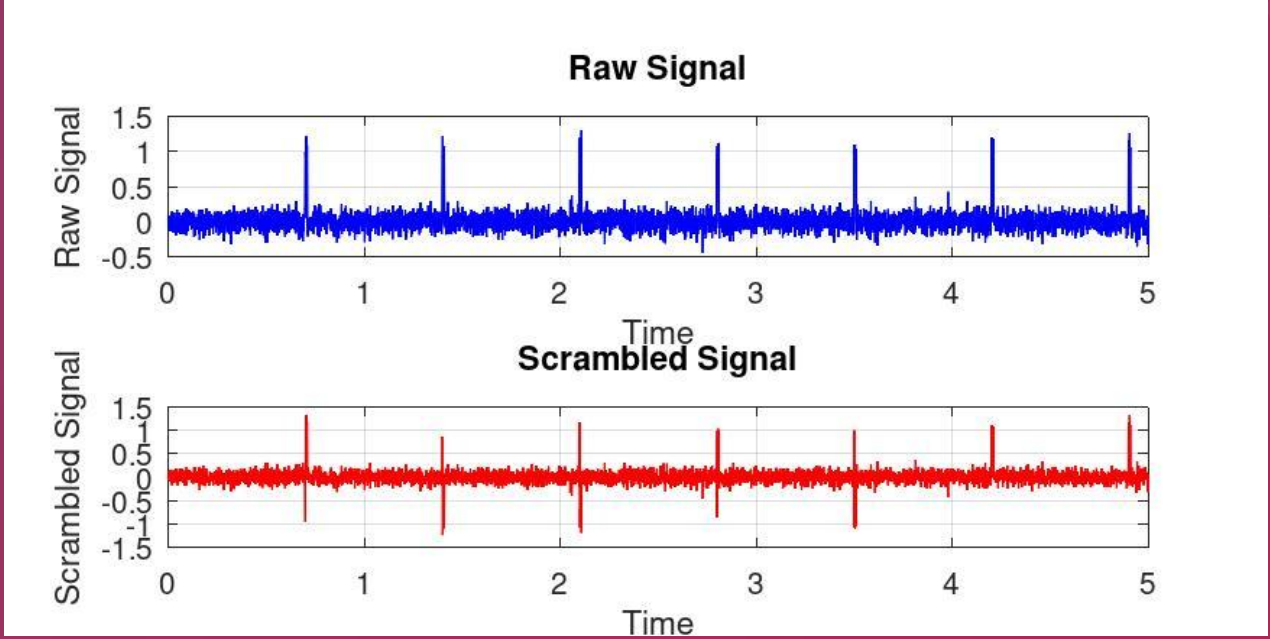
Project Purpose

- Model pulsar timing signals under realistic noise conditions to study detectability and leakage
- Scramble & descramble signals using cryptographic-style obfuscation to test signal integrity, and expose obfuscation secrets.
- Apply FFT, autocorrelation, and PSD to analyze periodicity and evaluate pulsar signals.
- Explore real-world applications: aerospace signal robustness and cybersecurity side-channel analysis

Pulsar Signal Obfuscation

- Uses seeded Mersenne Twister PRNG. Same seed & same call order reproduces sequence.
- Signal split into chunks, then scrambled via: flip/reverse, amplitude scale, and circular time shift
- Descrambling applies inverse steps in reverse. Correlation of raw and descrambled signal was 1.0, therefore recovery was lossless.
- Signal structure still partly detectable in visual inspection, but structure is more obscured in noisy time-domain environment.

Pulsar Signal Obfuscation

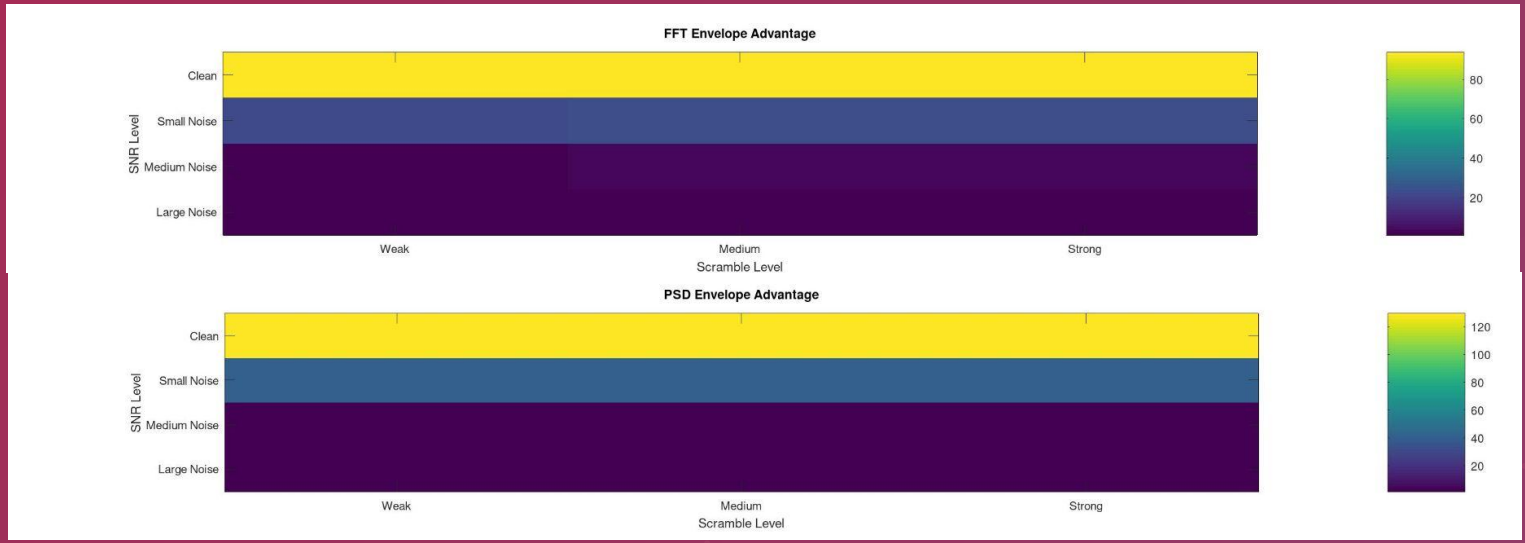


Pulsar Leakage Analysis - Spectral Fingerprinting

- FFT ratio and PSD ratio increased after scrambling, confirming that periodic structure remained detectable in the frequency domain.

Pulsar Leakage Analysis - Enveloping

- Applying hilbert envelope detection to capture instantaneous amplitude increased spectral leakage detectability compared to scrambled signals, particularly in low-noise environments.



Brute Forcing Neutron Stars

- Leakage analysis determined enveloping and spectral fingerprinting as the most effective in identifying the correct signal.
- Iterated through possible seeds and scrambling levels, descrambling the signal with the guessed seed, and scoring the descrambling success.
- score = (log-PSD ratio + log-FFT ratio) × envelope correlation coefficient
- Applied pre-filters (envelope with noise, PSD/FFT ×1.2) to balance metrics and reduce false positives

Attack Takeaways

- In small seedspaces, recovering the obfuscation PRNG seed had 100% top-1 accuracy.
- In time-domain scrambling routines, leakage can be effectively discovered through non-time domain analysis techniques.
- Despite scrambling routine's efforts, pulsars could often be discovered through visual inspection.
- This is useful in cases where an individual is without access to internal device architecture. Observation of signal patterns in the time-domain, correlations, or frequency signatures can reveal exploitable structures.

Defense Takeaways

- Brute forcing a 2^16 seedspace took ~40 minutes, a 2^128 seedspace would take ~0.4 nonillion years!
- Sufficiently large seed sizes make it computationally infeasible to brute force, even when the attacker has access to the encrypted data.
- Scrambling routines that use multiple blocks and can sufficiently alter the original signal shape are more effective in preventing data leakage.
- Low SNR reduced peak contrast, so by reducing ambient SNR on side-channels, there is a reduced risk in exposing sensitive information on devices.