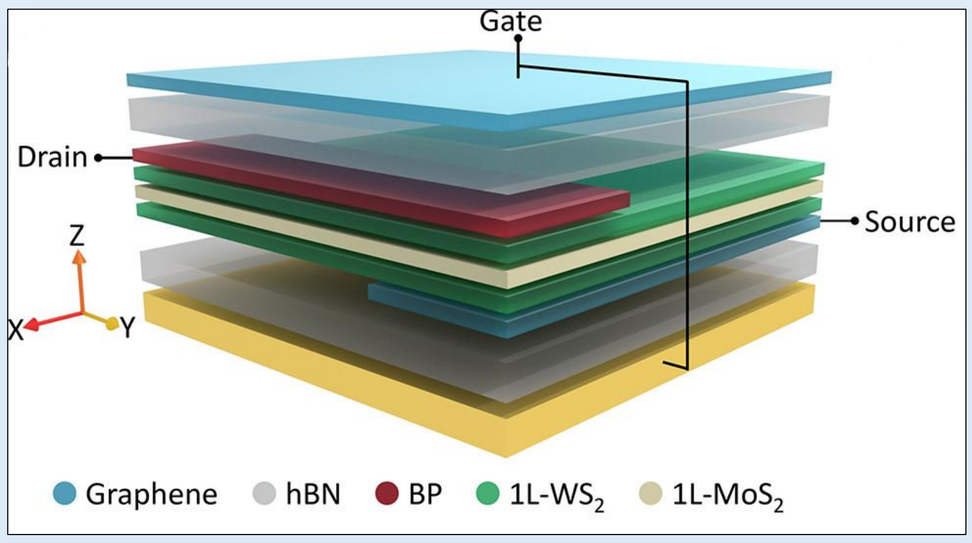
Development of high-quality random number generator for cyber security applications

CoE Objectives

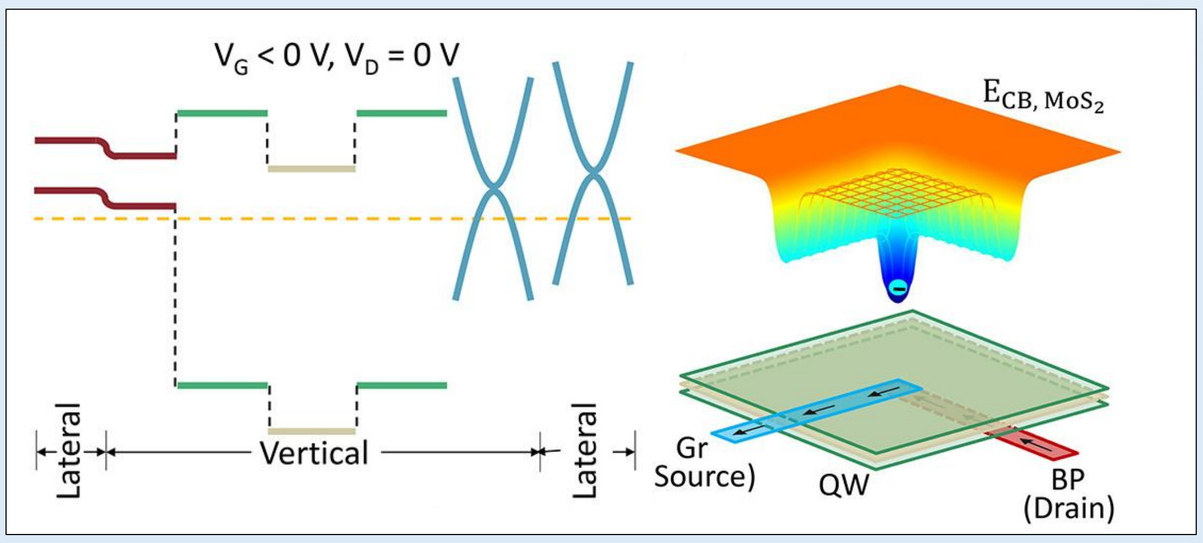
- Analyze cyber security issues in power transmission and grid operation
- Identify future cyber security challenges and provide mitigating measures

Project Objective

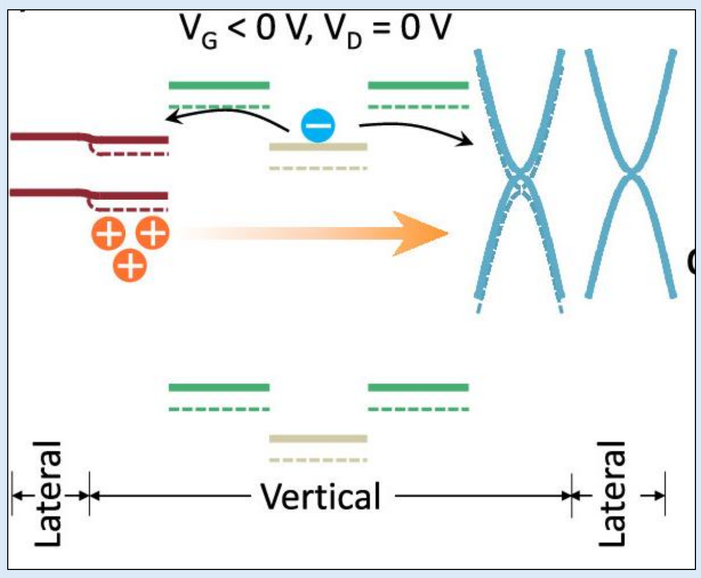
- Demonstration of high-quality random number generator device with min-entropy >0.98 bits/bit
- Integration of the fabricated device with signal processing circuit
- To generated sequence that is IID, which should pass NIST tests



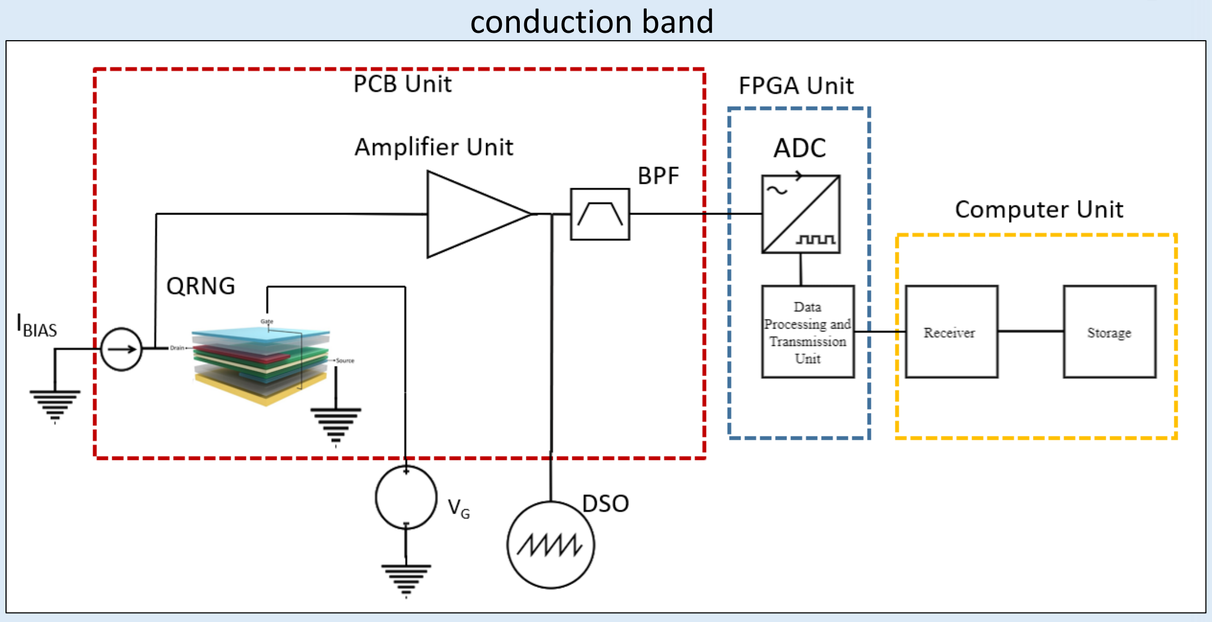
Fig(a): Device stack



Fig(b): Band alignment of the heterostructure & Schematic profile of the MoS_2 conduction band



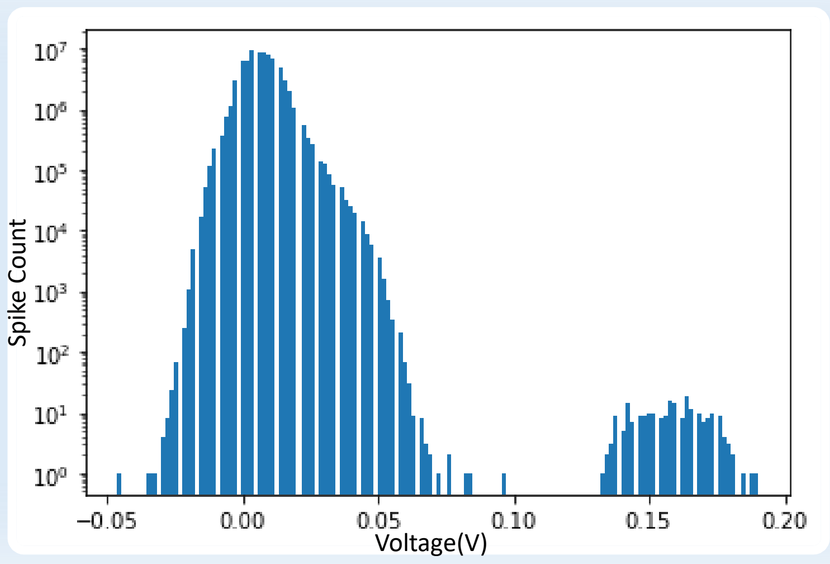
Fig(c): Generation of Signal



Fig(d): Data acquisition circuit

- The large conduction band offset between 1L-WS_2 and 1L-MoS_2 creates an electrostatic confinement in MoS_2 along the Z-direction.
- Entropy is embedded in the arrival time of the electrons in the trap.
- Time-to-digital conversion generates uniformly distributed 8-bit random symbols.
- De-trapping of electron by built-in field resets the device.

- The heterojunction stack design and optimization
- Initial batch of devices fabricated, with a detailed process optimization underway
- The first set of devices show clean voltage spikes above the noise level
- Data acquisition circuit design in progress



POWERGRID
CENTER OF EXCELLENCE
IN CYBER SECURITY

Ankit Gupta, Liza Jain, Sourav Das, and Kausik Majumdar

Quantum Electronics Laboratory