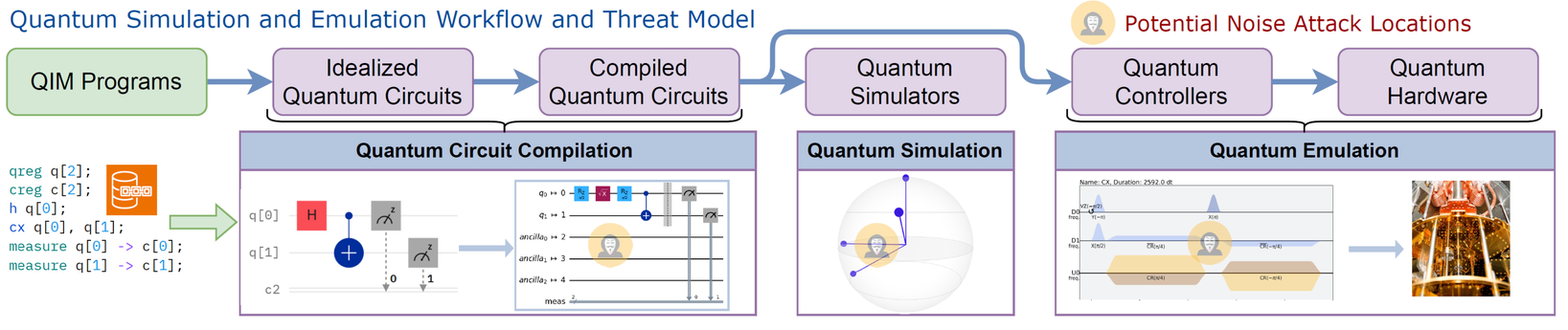
QURE: Usable and Attack-Resistant Security Framework for Quantum Emulators

PI: Qian Wang (UC Merced) Co-PIs: Lin Tian (UC Merced), Yuntao Liu (Lehigh University)

Systematic View of QURE

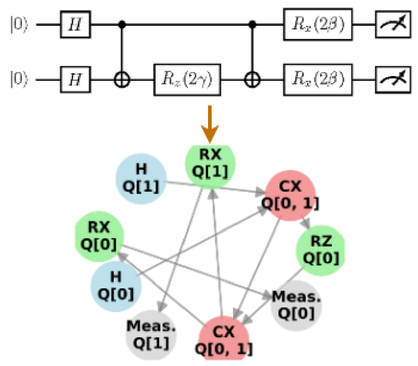


Collaboration and Usability Challenge Addressed

- Distinguishing **benign** noise and **adversarial** perturbations.
- Develop an **end-to-end security validation framework** for quantum emulation, integrating both **compile-time** and **runtime** protections.
- Build a **user-friendly sign-off software tool** so that physicists can adopt security checks without needing deep cybersecurity expertise.

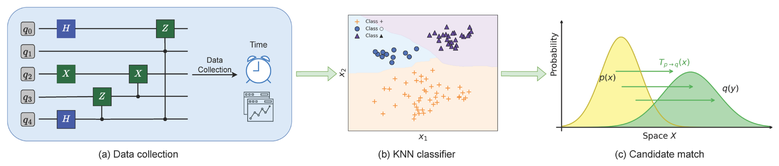
Technical Results and Solutions

Noise attack vulnerability prediction



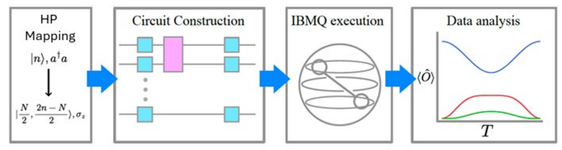
- Developed a GNN to predict noise injection impacts.
- Trained on quantum Ising models with added generic circuits.

ML-Based Classification of Noise and Timing Patterns in Quantum Simulators



- Demonstrated side-channel attack on cloud-based quantum simulators.
- Profiled timing and noise behavior enable circuit identification, achieved 88% to 99.9% circuit classification accuracy.

Digital quantum simulation for dynamics of quantum Ising model



- Demonstrated bosonic quantum simulation using the Holstein-Primakoff transformation on NISQ hardware with improved scalability and fidelity.
- Implemented harmonic oscillator and Jaynes-Cummings models, identifying key trade-offs among algorithmic and hardware errors.

Benefits to Scientific Cyberinfrastructure

Secure cloud-based quantum emulation
– ensures emulation platforms are secure, reliable, and trusted by scientific users.

Trustworthy scientific results
– reduces the risk of adversarial noise or attacks corrupting emulation outcomes.

Collaborative security validation
– establishes a collaborative security operations to enhance security validation efficiency for the scientific community.

Risks Versus Potential For Advances

Noise attack detection
– distinguishing between natural noise and adversarial perturbations is technically challenging

Cloud dependency
– evolving architectures of quantum platforms may limit access to low-level error data needed for robust validation.

Foundational security framework
– establishes first-of-its-kind tools for quantum emulator security, extendable to future quantum computing.

Result Dissemination Plans

- Demonstrated ability to **detect and mitigate adversarial attacks** on quantum emulation.
- Establishment of a **collaborative work** from quantum physicists and cybersecurity experts.
- Publication of **attack datasets, benchmarks, and detection scripts** on publicly accessible repositories.

GET the Published Preprints and Results