

Quantum Adversarial Variational Learning for FDIA Detection in Smart Grid Cyber-Physical Systems (QAVL-FD)

Pulluri Varshith, Undergraduate Researcher, EECS | Mentor: Dr. Ali Shiri Sichani, Asst. Teaching Professor, EECS | University of Missouri



Quantum Innovation Center
University of Missouri



Electrical Engineering
& Computer Science
University of Missouri

Abstract

False data injection attacks (FDIAs) can corrupt power-grid state estimates without triggering conventional bad-data detectors. We present five quantum and hybrid methods for generating and detecting such stealthy attacks, evaluated on IEEE 30/57/118-bus systems, 231,201 real CAISO measurements, and IBM Quantum hardware. Our Q-ASP-FDIA attacker achieves 100% attack success while remaining stealthy, and QB-DETECT achieves $F1 = 1.000$ against attacks that evade classical detectors.

Research Question Can quantum machine learning generate stealthy attacks that evade conventional detectors, and detect attacks that classical models miss?

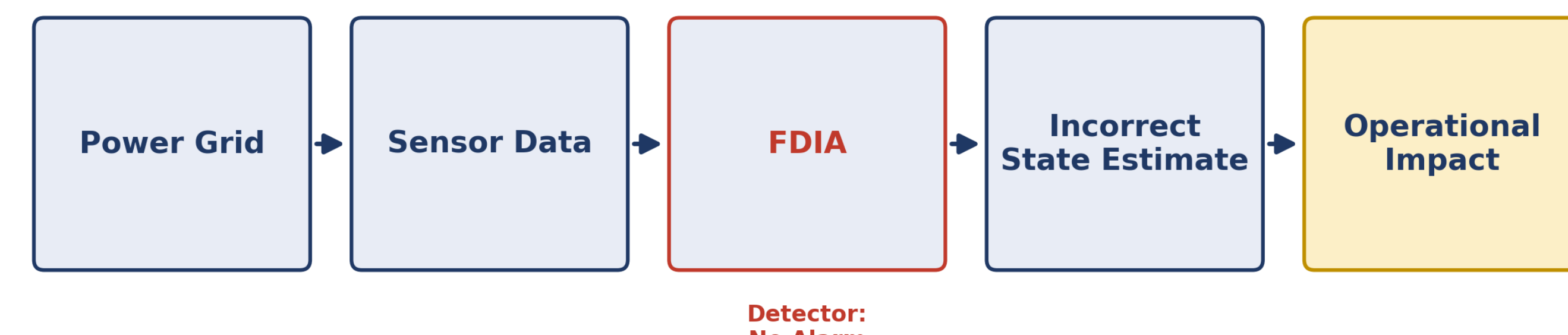


Fig. 1. FDIA pipeline: sensor measurements are manipulated to corrupt the grid state estimate, undetected.

FDIA (False Data Injection Attack): malicious manipulation of grid measurements designed to evade conventional detection.

Methodology

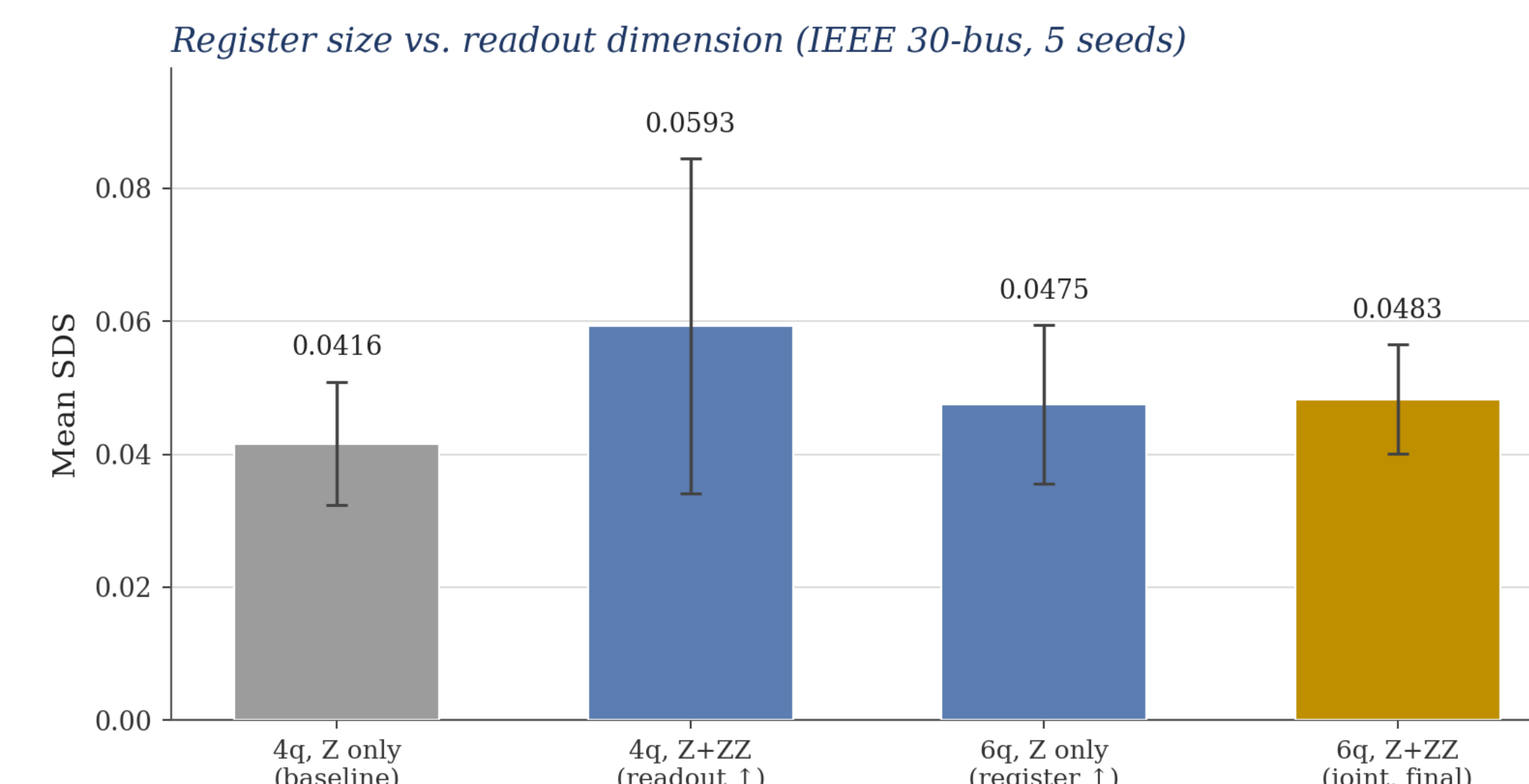
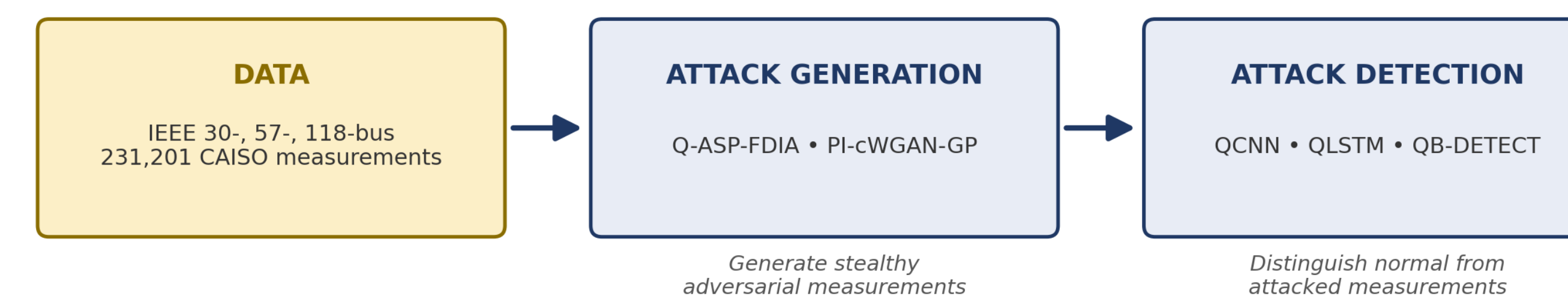


Fig. 2. Circuit ablation across register size and readout dimension (IEEE 30-bus, 5 seeds).

Circuit selection: Ablation experiments identified the 6-qubit Z+ZZ configuration used in the final Q-ASP-FDIA model.

Quantum Model Architecture

Parameterized quantum circuits were integrated with classical learning components for attack generation and detection.

QCNN Detector

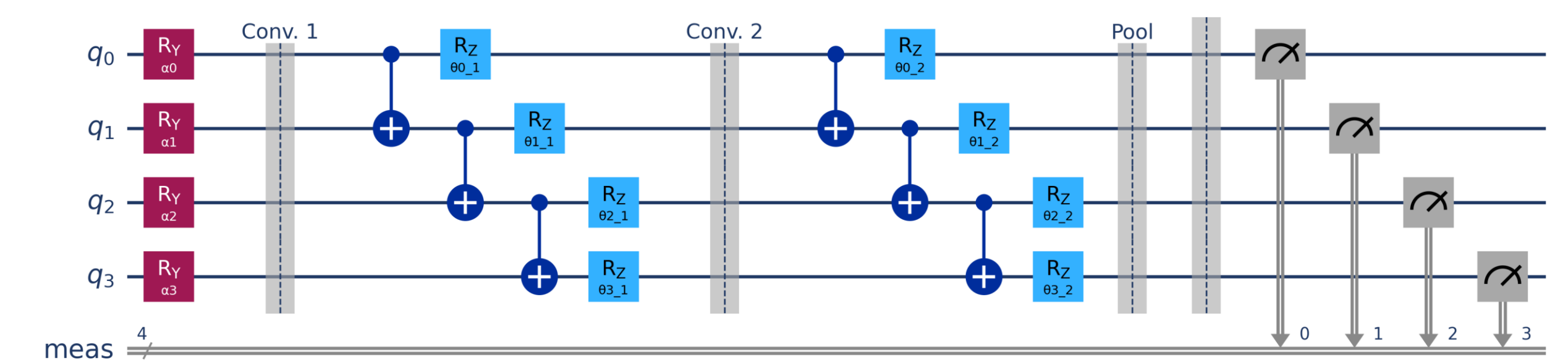


Fig. 3a. QCNN detector: 98.10% F1 in simulation, 75.52% on ibm_fez hardware.

Q-ASP Attacker

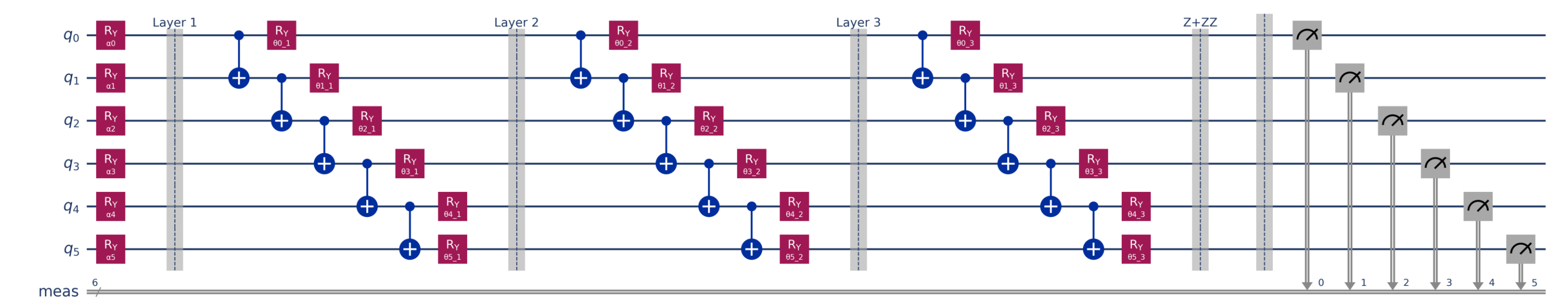


Fig. 3b. Q-ASP-FDIA attacker circuit (6 qubits, Z+ZZ readout).

Quantum component: Trainable circuit parameters encode and transform grid measurements before classification or attack generation.

Key Results

- Q-ASP-FDIA:** $ASR = 1.000 \pm 0.000$ across 10 seeds, with 3.8× smaller perturbations than the analytical baseline.
- Hardware validation:** 1,000/1,000 attacks remained stealthy during IBM Quantum evaluation.
- PI-cWGAN-GP:** Generated a 500,000-sample certified corpus with TSTR AUC of 0.76–0.90.
- QB-DETECT:** Achieved $F1 = 1.000$ on adaptive attacks missed by classical baselines.

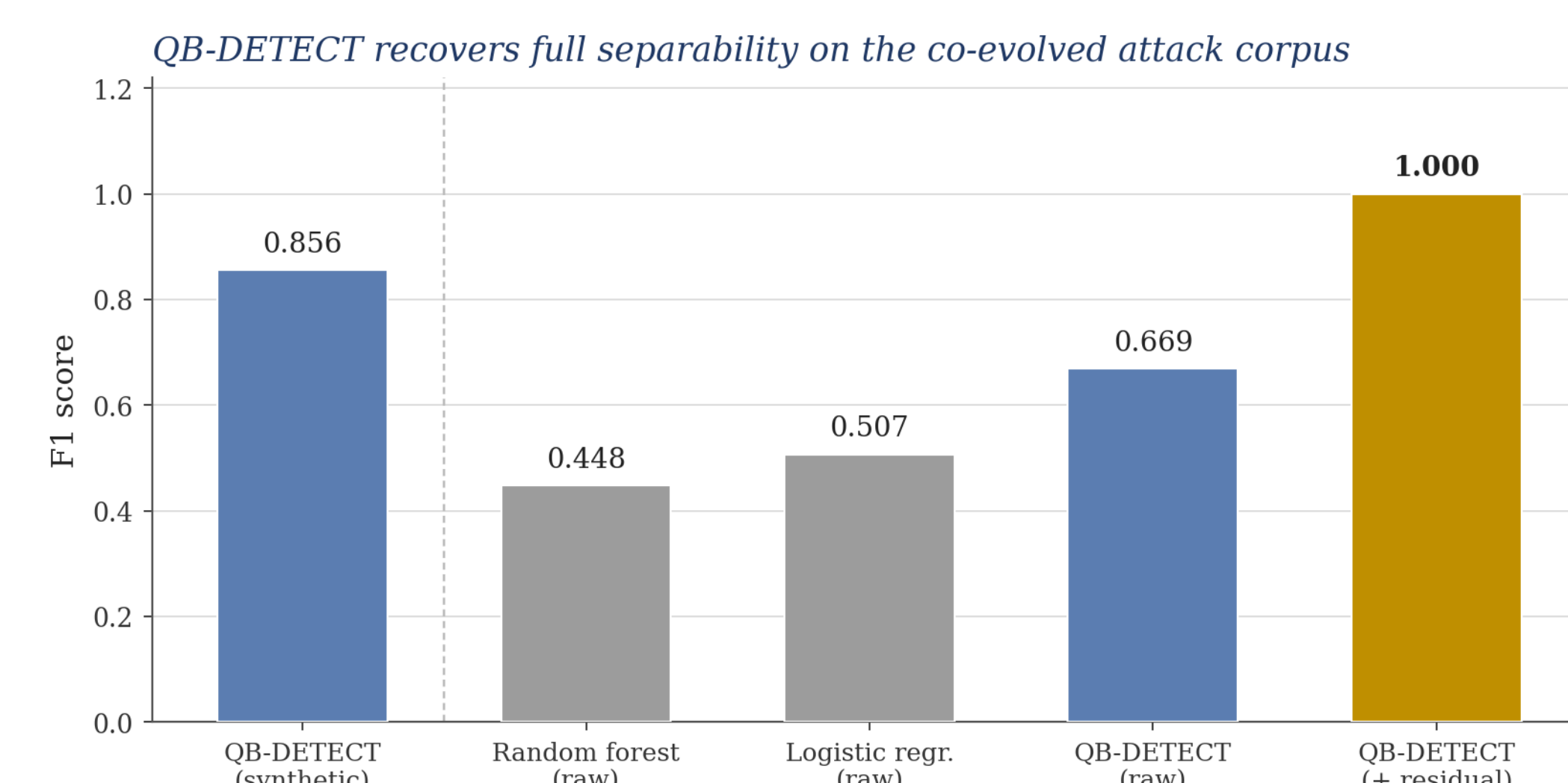


Fig. 4. QB-DETECT F1 on the Q-ASP co-evolved attack corpus vs. classical raw-measurement baselines.

Attack Performance Across Grid Scales

- Q-ASP-FDIA was evaluated across IEEE 30-, 57-, and 118-bus systems to examine attack success and stealth as system size increased.

Q-ASP-FDIA attack generation quality across IEEE bus systems

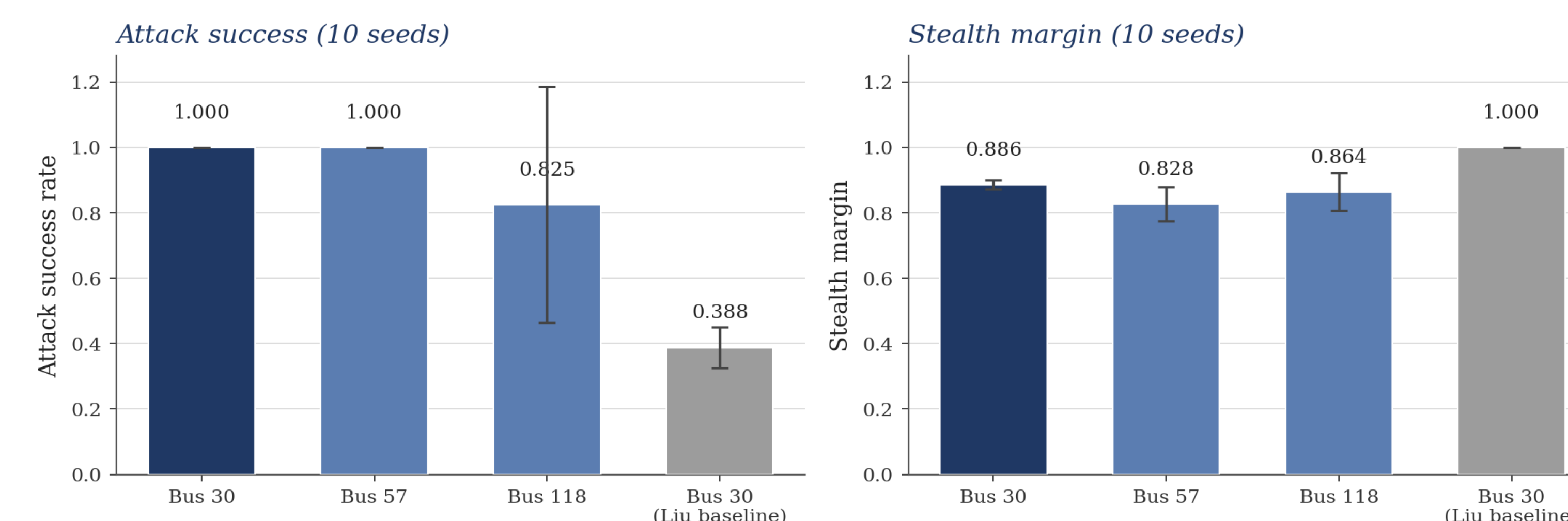


Fig. 5. Attack success rate and stealth margin across IEEE benchmark systems (10 seeds, mean $\pm$ SD).

Finding: Q-ASP maintained high attack success and positive stealth margins across all three benchmark systems.

Conclusions & Future Work

Conclusion:

- This study demonstrates quantum and hybrid approaches for both stealthy FDIA generation and detection across multiple IEEE benchmark systems. The models were further evaluated using real CAISO measurements and IBM Quantum hardware, extending the analysis beyond simulation.

Key Outcomes:

- Quantum advantage was not universal: the clearest gain appeared specifically against adaptive, co-evolving attacks (QB-DETECT), not static ones.
- The QCNN's gap between simulation (98.10% F1) and ibm_fez hardware (75.52% F1) reflects device noise and shot-limited sampling — a target for error mitigation, not a modeling failure.
- Perfect scores ($ASR = 1.000$, $F1 = 1.000$) reflect a matched threat model where the detector trains on the same co-evolving attacker; robustness to unseen attack families remains untested.

Future Work

- Future work will investigate when quantum generative models provide measurable advantages over matched classical methods and evaluate scalability to larger power-system datasets and hardware.

[1] Khaliq, Alla, Pulluri, et al., "Quantum ML for Localizing Stealthy FDIAs in Power Grids," Proc. 58th NAPS, 2026.

[2] Khaliq, Alla, Pulluri, et al., "When Does Quantum Generation Help?" manuscript in prep., target: Nature Communications, 2026.

Supported by Mizzou QIC, the IBM Quantum partnership, and Hellbender HPC.