Classification of Security Challenges and Mitigation Approaches in the QSE

Background & Motivation

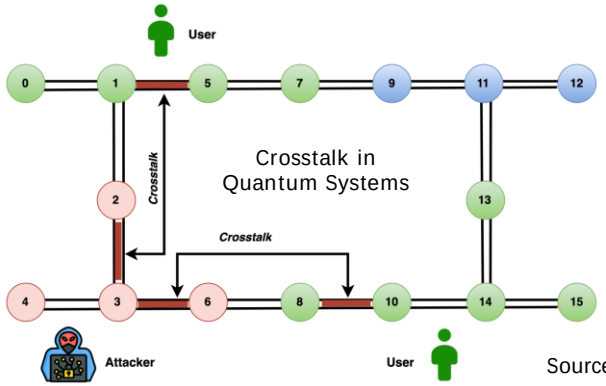
QPA Research Group

- Multi-tenant cloud platforms face emerging security threats (Crosstalk, Side-Channel, Fault-Injection, Pulse-Level attacks) that are addressed in a fragmented way in existing studies.
- Current literature about mitigation approaches for the mentioned security threats lack comprehensive analysis and mapping between attacks families and different security aspects of mitigations.
- In this work, we provide an organized view of towards security threats and their mitigation techniques of QSE by furnishing a classification of the security threats with examples and aligned comparative mitigation approaches across different levels (Maturity Level, Scalability, Hardware dependency).

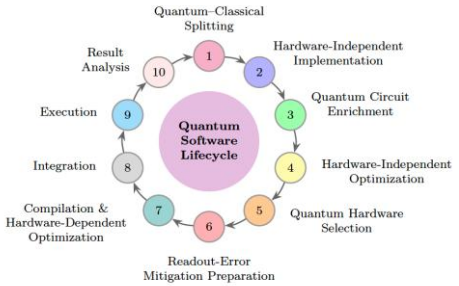
Rahman, B., Haghparast, M., & Mikkonen, T. (2026). Classification of security challenges and mitigation approaches in the quantum software engineering. *Journal of Systems and Software*, 112884.

https://doi.org/10.1016/j.jss.2026.112884

Proposed Research Item and Goal



Source: Choudhury, 2024



Source: Wader, 2020

Overview of the Quantum Software Lifecycle

- Classification of security threats into four families of Quantum Software Engineering
  - Crosstalk: Operational Crosstalk, Idling Crosstalk Double-sided Crosstalk, Qubit-Flipping attacks.
  - Side-Channel: Power Side-Channel, Timing Side-Channel, Quantum Side-Channel, Hybrid Side-Channel.
  - Fault-Injection: QPU Faults, Controller Faults, Auxiliary Processor Faults
  - Pulse-Level: Channel Attacks, Pulse Attacks, Compound Attacks
- Overview Of The Study

  4 Attack Families → 14 Attack Classes → 30+ Mitigation

▸ GOAL: Establish structured and unified bridge between attack classification and mitigation assessment. ◂