

An End-to-End Threat Model for the Quantum-as-a-Service Pipeline

Background & Motivation

QPA Research Group

- Cloud **QaaS** platforms (IBM Quantum, IonQ Cloud, Amazon Braket) expose quantum processors behind classical APIs, and hybrid algorithms (VQE, QAOA, QML) traverse a long, layered pipeline.
 - Critical attacks are demonstrated per stage, such as **SWAP attack**, **QubitHammer**, **Inverse-transpilation**, **Calibration tampering**, **Pulse abuse**, yet each stays siloed under its own terminology.
 - Existing STRIDE work targets classical cyber-physical systems or quantum attacks on classical cryptography.
- No unified service-level threat model exists for the QaaS stack itself.**

Rahman, B., Haghparast, M., & Mikkonen, T. (2026). An End-to-End Threat Model for the Quantum-as-a-Service Pipeline. *arXiv preprint arXiv:2608.05836*.

<https://arxiv.org/abs/2608.05836>

Proposed Research Item and Goal

Six-Stage QaaS Pipelines



STRIDE × Stage Attack-Surface Matrix

Stage	S	T	R	I	D	E
S1 Dev.						
S2 Auth						
S3 Compile						
S4 QPU						
S5 Return						
S6 Loop						

S Spoofing · T Tampering · R Repudiation · I Info. disclosure · D DoS · E Elev. of privilege

Published attack Inherited classical Plausible

- Six-stage STRIDE threat model**
 - ❖ **S1** Developer Environment (SDK simulation)
 - ❖ **S2** Authentication & Submission (API token, IAM)
 - ❖ **S3** Orchestration & Compilation (queue, transpiler)
 - ❖ **S4** Hardware Execution (calibration metadata, pulse control, multi-tenancy)
 - ❖ **S5** Result Return Path
 - ❖ **S6** Hybrid Iteration Loop (repeats S2–S5)
- Repudiation** is under-studied at every stage, elevation-of-privilege is published only at S4.
- Three cross-stage attack chains**
 - **A** - Side-channel ID → targeted crosstalk
 - **B** - Calibration topology → pulse placement
 - **C** - Compiler IP leak → transpile-stable Trojan
- Overview Of The Study**
6 Stages × 6 STRIDE Categories → 3 Attack Chains

► **GOAL: Unify siloed QaaS attacks into one service-level attack-surface map.** ◀