Quantum Computing Threat Landscape

Author: Markku Kylänpää

Overview

Quantum computing represents a fundamentally new computing paradigm with the potential to transform a wide range of fields, including cryptography, simulation, and optimization. To date, most security efforts have focused on the potential threat that quantum algorithms pose to asymmetric cryptographic schemes. However, the security considerations extend beyond cryptographic vulnerabilities. Because quantum computing is predominantly delivered as a cloud-based service, platform-level security introduces additional risks, including threats related to multi-tenancy, data isolation, and system integrity.

System model

Clients typically access quantum computers through cloud-based services. The quantum processing unit (QPU) and its control hardware present multiple opportunities for monitoring and side-channel observation, particularly for adversaries with physical access to the system.

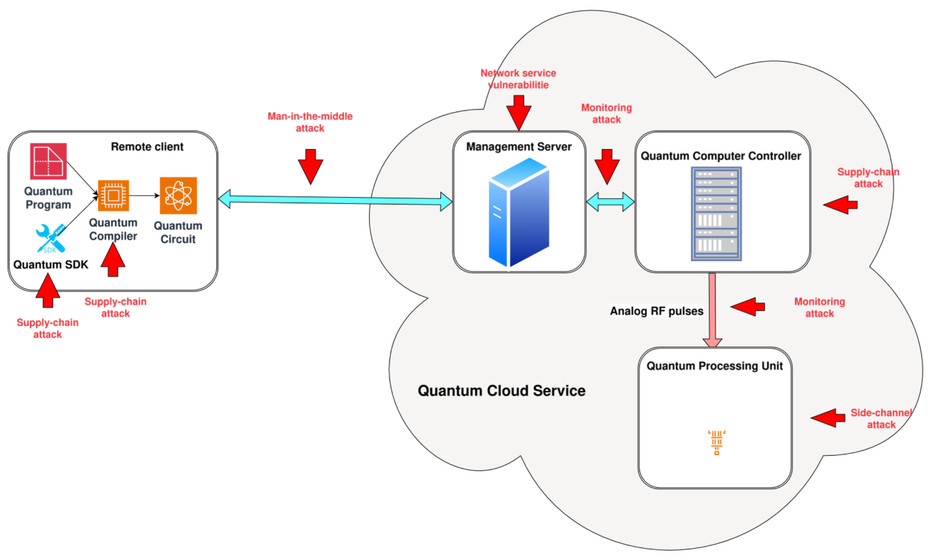

Figure 1. System architecture

Adversary model

Clients utilizing quantum computing services may be exposed to several potential adversaries:

- **Honest-but-curious cloud service provider**: The quantum cloud provider may passively observe customer workloads through various system-level monitoring mechanisms, potentially gaining insights into sensitive computations.
- **Malicious co-tenant client**: Although large-scale multi-tenancy is not yet widely deployed in quantum systems, its future adoption could introduce risks where a malicious client leverages shared infrastructure to monitor or interfere with other clients' operations.
- **Supply-chain adversary**: Entities involved in the hardware, software, SDK, or compiler supply chain may have opportunities to access or infer proprietary client information, posing risks to confidentiality and intellectual property.

Threat categories

The following table provides a high-level classification of attack types, organized into four categories, along with brief descriptions of their potential impact.

Table 1. Threat category examples

Threat category	Example attacks	Primary impact
Side-channels	Timing, power, readout, crosstalk leakage	Circuit and data confidentiality loss
Multi-tenancy	Crosstalk exploitation, reset leakage, DoS	IP theft, integrity and availability risks
Pulse-level attacks	Timing, frequency, waveform manipulation	Incorrect computation, decoherence
Supply chain	Malicious compilers, SDKs, hardware Trojans	Stelthy long-term compromise

Integration of classical and quantum computing

Quantum computers are increasingly used in conjunction with classical systems, often serving as specialized accelerators for targeted computational tasks. In this hybrid model, classical high-performance computing (HPC), GPUs, and QPUs are integrated to complement each other's strengths. Confidential quantum cloud computing must evolve to support such hybrid architectures, ensuring secure and efficient orchestration across heterogeneous computing resources.

Establishing trust in remote quantum computing platforms

Confidential quantum cloud computing services must provide strong guarantees of both integrity and confidentiality across QPU-enabled environments. Achieving this requires robust mechanisms for remote attestation and reliable device identification, ensuring that clients can verify the authenticity and state of the underlying hardware and control systems. However, the unique characteristics of quantum platforms introduce new challenges: communication between the controller and QPU relies on analog RF signals, which are inherently difficult to conceal or obfuscate and may expose side-channel information. To mitigate these risks, enhanced physical security measures, such as tamper-resistant or tamper-evident packaging, are likely necessary to protect sensitive components and maintain trust in the platform.

Conclusion

Practical and scalable mechanisms are needed to establish trust in remote quantum computing platforms. As QPUs are increasingly integrated with classical systems, hybrid computing frameworks combining HPC, GPUs, and quantum resources will become the norm. Ensuring a secure quantum supply chain is essential to protect both hardware and software components. Additionally, the introduction of multi-tenancy expands the threat landscape, as co-located clients may act as potential adversaries.

Contact: Markku Kylänpää, Senior Scientist
Tel. +358 40 546 4427, markku.kylanpaa@vtt.fi