Vulnerabilities of the Reset Operation on Superconducting Qubits

Sorin Bolos
Adrian Colesa, Radu Mărginean

Transilvania Quantum, str. Victor Hugo nr. 21, Cluj Napoca, Romania

sorin.bolos@transilvania-quantum.com

The impact of quantum computing on classical cybersecurity has been discussed extensively over the past 30 years, leading to the development of post-quantum cryptography. At the same time, relatively little attention has been paid to the security of quantum computers themselves.
The little research that studied vulnerabilities of quantum computers until now has focused on a scenario where circuits belonging to different users are executed on the same quantum chip at the same time. [1][2] This mode of operation is not yet in possible.
We focused on vulnerabilities of superconducting QPUs that are available today.
We conducted two experiments on the ibm_osaka quantum chip where we leveraged the imperfections of the reset operation, and we show that: (1) an attacker can infer the final state of the circuit that ran before him, stealing the results of the computation. (2) an attacker can leave qubits in a higher excited state so that the circuit that runs after him will start in a state that is not the ground state, compromising the results.

References

[1] S. Deshpande et al., 2022 IEEE International Symposium on Hardware Oriented Security and Trust, 2022, Pp. 37–40.
[2] A. Ash Saki et al, arXiv: 2106.06081
[3] A. Mi, S. Deng, J. Szefer, CCS '22: Proceedings, 2022, Pp. 2279–2293
[4] A. Ash Saki and S. Ghosh, arXiv: 2104.05899, 2021

Figures

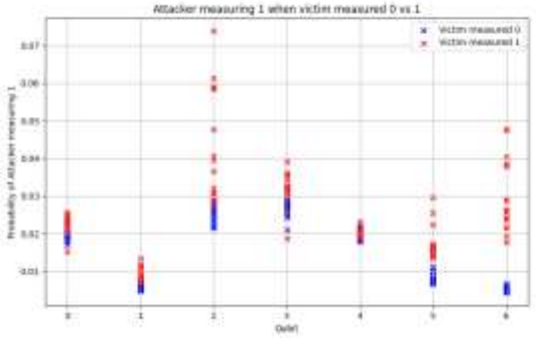

Figure 1: Attacker measuring '1' when victim measured '0' vs '1'.

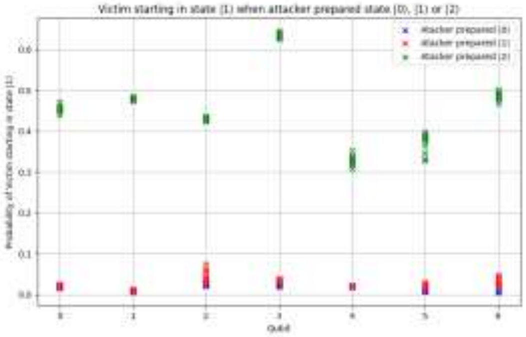

Figure 2: Probability of victim qubits starting in state |1⟩ when the attacker has prepared the qubits in state |0⟩, |1⟩, or the second excited state (|2⟩).