

University of Michigan,
Ann Arbor, MI, 48105

April 10, 2023

Nomination Letter for paper “Securing Reset Operations in NISQ Quantum Computers”

Dear Members of the Evaluation Committee,

It is with great enthusiasm that I nominate paper “Securing Reset Operations in NISQ Quantum Computers” published in CCS 2022 for consideration for the 11th Annual Best Scientific Cybersecurity Paper.

This paper examines the issue of information leakage in quantum computers utilized in a shared cloud-based environment, focusing on reset operations. They demonstrate two attacks: 1) information leakage across resets, and 2) information leakage due to crosstalk-like behavior. The authors simulate these attacks on IBM Cloud’s actual quantum-computing hardware and highlight the limitations of fast primitives and their inability to fully reset quantum states, leading to information leakage. Furthermore, the paper also explores the impact of crosstalk effects on information leakage and discusses potential mitigations by developing secure reset operations. The proposed scheme achieves higher security and fidelity than a full-system wipe while delivering a significant speedup of approximately 300 times. It brings about quantum computer multi-tenancy and makes quantum computers more accessible to a broader user base.

The key insight of this work is to speculatively study the security of reset operations and fix any problems we can anticipate for the security of this upcoming technology, namely quantum computers. Quantum computers have the potential to revolutionize computing by exploiting the principles of quantum mechanics to perform calculations faster and more efficiently than classical computers. With that, the security of the prospective or novel reset methods, should they come to exist, should be the focus of the additional and independent investigation. The examination and validation of critical enabling components’ security should not be deferred until complete quantum computer multi-tenancy is made commercially available, as considering security only at that point would have adverse consequences.

Besides that, this work has the following detailed key contributions which make it deserving of the award: 1) The paper presents a novel idea for attacks that could compromise the security of quantum computers when used in a shared, cloud-based setting. The proposed attacks aim to exploit the imperfections in the reset operation of qubits, which can lead to information leakage across different users and programs. 2) To demonstrate the viability of these attacks, the authors executed simulations on actual quantum computing hardware provided by IBM Cloud. This provides a realistic testbed to assess the proposed attacks’ effectiveness and evaluate the potential impact of information leakage, adding weight to the study’s findings. 3) The techniques described in this study are potentially transferable to other quantum computers. The proposed model and methodology are solely based on the gate-based description of the reset operation. Therefore, as long as the reset is executed by measuring and subsequently conditionally flipping the quantum state, this approach could be extended to other superconducting devices, or conceivably to other categories of quantum computers as well.

All things considered, I would like to nominate this paper for the Annual Best Scientific

Cybersecurity Paper award. If there is anything else I can do to support, please do not hesitate to contact me.

A handwritten signature in black ink, appearing to read 'Kasikci', with several horizontal lines to its left.

Sincerely yours,
Baris Kasikci, Morris Wellman
Assistant Professor
Department of Electrical Engineering
and Computer Science
Phone: +1 (734) 763-1560
Email: <mailto:barisk@umich.edu>
Web:
<https://web.eecs.umich.edu/~barisk/>