University *of*
Massachusetts
Amherst

College of Engineering

Dean's Office

Russell Tessier
(413) 545-6454 voice
(413) 545-0724 fax
tessier@umass.edu

March 25, 2023

11th Annual Best Scientific Cybersecurity Paper Competition Selection Committee,

It is my pleasure to nominate the work by Mi et. al for the NSA's Best Science of Cybersecurity paper competition. The work by Mi et. al is the first major research paper published at the Conference on Computer and Communications Security (CCS) on the subject of security of quantum computers. The work was published in November 2022.

The NSA's Best Science of Cybersecurity paper competition has in the past recognized breakthrough papers on important, future-looking security problems. With the emergence of quantum computing as a game-changing field of research, it is necessary to secure these novel types of computers. Security research cannot only focus on classical computers. Work by Mi, et. al advances the scientific foundations of cybersecurity in this new realm of quantum computers.

Quantum computers are crucial for enabling next-generation compute capabilities in scientific research, drug discovery, finance, machine learning, and many other fields. The quantum computing industry is valued at USD $712.2 million in 2022. The reset operation is a critical component in quantum computers. With reset, qubits can be re-initialized much faster (on the order of 10us) than thermalization (on the order of 500us). Showing how to securely reset qubits can enable much faster quantum computation and utilization of the quantum computers, since they do not have to stay idle waiting for qubits to thermalize.

The secure reset presented by Mi et. al is an enabling technology for secure and robust quantum computers, and thus has significant potential for economic benefits and security of critical quantum computing infrastructures. The novelty of the solution lies in both the simplicity and effectiveness of the design. Further, it requires no hardware modifications to existing quantum computers, making this a new technology that can be adopted today. The secure reset leverages well-known principle of confusion to confuse potential adversaries. Current (insecure) reset leaks information allowing adversaries to learn the state of the qubit prior to the reset. With secure reset, randomization is introduced. A random number of reset operations is performed in sequence, one of two random sequences is chosen with probability p and 1-p, respectively. Although an adversary is still able to measure some information, they cannot correlate the measured qubit state to the state of the qubit prior to reset, effectively eliminating any information leakage.

I give this paper my highest recommendation for the award.

Sincerely,

Russell Tessier

Russell Tessier
Senior Associate Dean, College of Engineering
Professor, Department of Electrical and Computer Engineering
University of Massachusetts Amherst
tessier@umass.edu