Nomination for Science of Security Paper Competition 2025

Nominated Paper:

Space-Efficient and Noise-Robust Quantum Factoring
by Seyoon Ragavan and Vinod Vaikuntanathan

Published in Crypto 2024.
Winner of Best Paper Award at Crypto 2024.

paper: https://eprint.iacr.org/2023/1501
talk: https://www.youtube.com/watch?v=pCP9gRKS7sI

Shor's seminal quantum factoring algorithm had a dramatic impact on developments in cryptography and quantum computing. Recently, an alternative algorithm was proposed by Regev, which reduced the number of gates but increased the number of qubits. This paper (which won the Best Paper award in Crypto 2024), improves on Regev's algorithm, reducing the number of qubits needed and also adding noise-robustness.