香港科技大學(廣州)
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

Tensor Network Attack on Cryptographic Protocols

A paper review

Yusheng Zhao

HKUST(GZ)

2024-11-07

香港科技大學(廣州)
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

Outline

香港科技大學(廣州)
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

Outline

Improved Variational Quantum Attack Algorithm on Cryptographic Protocols

1. Reduced number of qubits and circuit depth
2. Used coordinate transformation to reduce Barren Plateau
3. Generalized this approach to work with symmetric and assymetric key encryption.

Encodes a known ciphertext as the ground state of a classical Hamiltonian.

How can I do encoding without knowing the ground state? How does secret key correspond to variational parameter for the ground state of this classical Hamiltonian?

香港科技大學(廣州)
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

Outline

Assumes know the plain text and corresponding cipher text, want to extract the secret key.

What is the benefit of using tensor network? It is not faster! Only fewer iterations. Why should we care about the number of iterations if the total time is longer?

"More complex the cipher and the longer the key, the more compelx the best hacking method is." [2], in what sense is VQAA more complex than MPS approach?

Bibliography

[1] B. Aizpurua, P. Bermejo, J. E. Martinez, and R. Orus, "Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks," *arXiv preprint arXiv:2311.02986*, 2023.

[2] B. Aizpurua, S. Patra, J. E. Martinez, and R. Orus, "Hacking Cryptographic Protocols with Tensor Network Attacks," *arXiv preprint arXiv:2409.04125*, 2024.