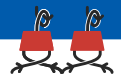
# Tensor Network Attack on Cryptographic Protocols

## A paper review



Yusheng Zhao

HKUST(GZ)

2024-11-11

# New paper

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?

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.” [1], in what sense is VQAA more complex than MPS approach?

Ok, there’s the trend in Table III and Table II, but did they give explaination to why we observe this?

Using MPS to represent probability distribution has two advantages [2]:

1. Stronger learning ability that grows with bond dimension (why? it is because of the vast amount of states representable by MPS with growing bond dimension and the efficient way of contracting MPS for computing probability distribution?)

2. More efficient sampling method (how?)

# Bibliography

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

[2] Z.-Y. Han, J. Wang, H. Fan, L. Wang, and P. Zhang, "Unsupervised Generative Modeling Using Matrix Product States," *Phys. Rev. X*, vol. 8, no. 3, p. 31012–31013, Jul. 2018, doi: 10.1103/PhysRevX.8.031012.