

Contribution ID: 85

Type: Talk

Tensor Network approach for factoring RSA numbers

Wednesday 8 May 2024 14:30 (30 minutes)

Current public-key cryptography standard is based on the RSA algorithm [1], whose security relies on the practical difficulty of factoring semiprimes as the product of two large prime numbers. While traditionally applied for encryption, lattice-based cryptography, as exemplified by Schnorr's algorithm [2], offers a different avenue to decompose RSA keys. This algorithm encodes prime factors into optimal solutions of NP-hard mathematical lattice problems, specifically the closest vector problem (CVP). However, the inherent difficulty in solving CVPs, even for moderately sized RSA integers, hinders efficient factorization.

A recent alternative approach [3] encodes optimal CVP solutions into low-energy eigenstates of a spin-glass Hamiltonian. Leveraging tensor network (TN) methods for extensive simulation of many-body systems [4], we present a quantum-inspired approach to efficiently extract optimal solutions from these CVP spectra.

We report a systematic numerical analysis of our TN-factoring method and we factorize RSA semiprimes up to more than 100 bits. This is the largest RSA number reached with Schnorr's sieving method to date. Moreover, we present a detailed resource assessment for targeting cryptographic keys of hundreds of bits on a standard cluster. Finally, we discuss the extrapolation of these findings towards the widely adopted RSA-2048 cryptosystem. Our TN approach provides insights into the practical implications of Schnorr's latticebased quantum algorithm, contributing to the ongoing discussion on cryptographic security in the context of emerging quantum computing methodologies.

References

[1] R. L. Rivest et al., A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21 (2) (1978), pp: 120-126

[2] C. P. Schnorr, Fast Factoring Integers by SVP Algorithms (corrected), Cryptology ePrint Archive (2021), 933
[3] B. Yan et al., Factoring integers with sublinear resources on a superconducting quantum processor, arXiv (2022), 2212.12372

[4] S. Montangero, Introduction to Tensor Network Methods: Numerical simulations of low-dimensional manybody quantum systems, Springer (2018), 978-3-030-01409-4

Presenter: TESORO, Marco (Univesità di Padova)

Session Classification: Talks