Interesting Quantum Information Science articles

Sahar Saoudi

November 2, 2023

1 Subject

All of these articles mentioned below are articles I found in the university of Sherbrooke's Inspec. The latter is a database of articles from periodicals, conference proceedings, and technical reports primarily in the fields of computer science, electrical engineering, computer engineering, electronics, and physics. I was doing research on the algorithm of Shor and I came across these articles. Each one of them talks in some way about the algorithm of Shor and all of them are super interesting ! For context, Shor's algorithm, devised by Peter Shor, is a quantum algorithm that efficiently factors large integers into their prime components, posing a threat to classical cryptographic systems relying on the difficulty of factoring for security. By leveraging quantum parallelism, Shor's algorithm achieves exponential speedup over classical factoring algorithms, potentially compromising widely-used cryptographic protocols.

2 Article 1

- Quantum Binary Field Multiplication with Optimized Toffoli Depth and Extension to Quantum Inversion †
- Jang, K., Kim, W., Lim, S., Kang, Y., Yang, Y., Seo, H.
- 2023
- Sensors, Page 3156 (14 pp.)

reference: [**23442639**]

2.1 Description

Shor's algorithm addresses the discrete logarithm problem on binary elliptic curves, but its quantum implementation faces challenges, notably the overhead of binary field arithmetic. This study focuses on optimizing quantum multiplication, adopting the Karatsuba method to reduce both Toffoli depth and full depth. The proposed approach achieves a Toffoli depth of one, lowers the overall circuit depth, and demonstrates superior trade-off performance in resource

requirements. This optimized quantum multiplication is particularly effective when integrated into algorithms like the Itoh-Tsujii inversion.

3 Article 2

- Quantum Optimization for Linear Algebra Problems
- Borle, Ajinkya
- 2022
- ProQuest Dissertations and Theses Global

reference: [**20230513513456**]

3.1 Description

This dissertation delves into the era of noisy intermediate-scale quantum (NISQ) computers, acknowledging their limitations for traditional algorithms like Shor's or Grover's. It explores the potential of NISQ-era quantum optimization, focusing on quantum annealing for solving linear least squares problems and gate-model quantum approximate optimization algorithms (QAOA) for linear algebra. The study reveals that quantum annealing can outperform classical methods for certain conditions, particularly in densely connected linear algebra problem graphs. Post-processing techniques, such as single-qubit correction (SQC), prove effective in improving solution quality, especially in densely connected domains. The dissertation also investigates the application of QAOA for binary linear least squares (BLLS), showcasing its scalability for good approximate solutions, although optimal solutions remain challenging. Simulated Annealing is found to outperform QAOA for BLLS under specific conditions. The work underscores the possibilities and challenges of applying quantum optimization in the NISQ era, emphasizing the practical aspects of quantum-classical hybrid solvers and pointing out current challenges in experimental implementations.

4 Article 3

- Quantum technology's role in cybersecurity
- Teodoras, D.-A., Popovici, E.-C., Suciu, G., Sachian, M.-A.
- 2023
- Proceedings of SPIE, Page 124930G (8 pp.)

reference: [**23251628**]

4.1 Description

In the realm of quantum technology development, Shor's algorithm has compromised most asymmetric encryption, while symmetric algorithms like AES-256 remain resilient against quantum attacks, with Grover's algorithm merely halving brute force attack time. This paper suggests exploring the impact of quantum technology on existing security algorithms and proposes the development of new encryption methods to enhance data protection. Quantum cryptography, particularly through Quantum Key Distribution, introduces the potential for revolutionary advancements, offering solutions to cryptographic challenges currently deemed insurmountable by classical computers. Lastly, the paper explores how the concept of quantum teleportation could usher in faster and more secure telecommunication solutions compared to those relying on traditional radio technologies.