QC @ SC

An Overview of cooperation with CQTA Zeuthen

Lukas Mansour

FH Scientific Computing Workshop,

Hamburg, 01.07.2024

Overview

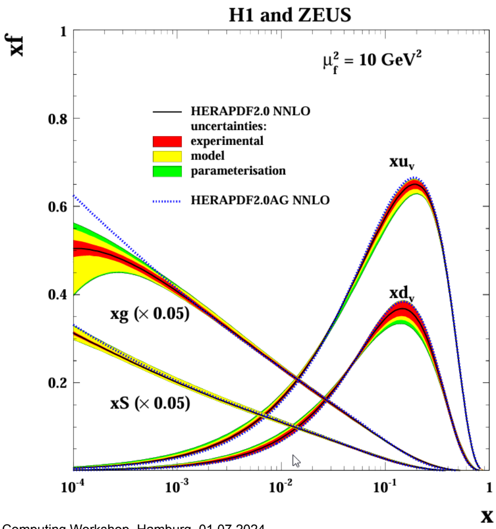
- Overview of Projects
- Possible QC Usecases in SC

Project #1: PDFs using Quantum Computers

- Calculate Parton Distribution Functions using QC.
- In 2+1 Dimensions.
- One Day in the Future: Compare a 3+1 calculation to results from a H1-Zeus cooperation.

Topics: State Preparation, State Evolution, Hadronic State mapping, Variational Algorithms, Encoding Schemes, Lattice Theories, Hamiltonians

Project #1: PDFs using Quantum Computers



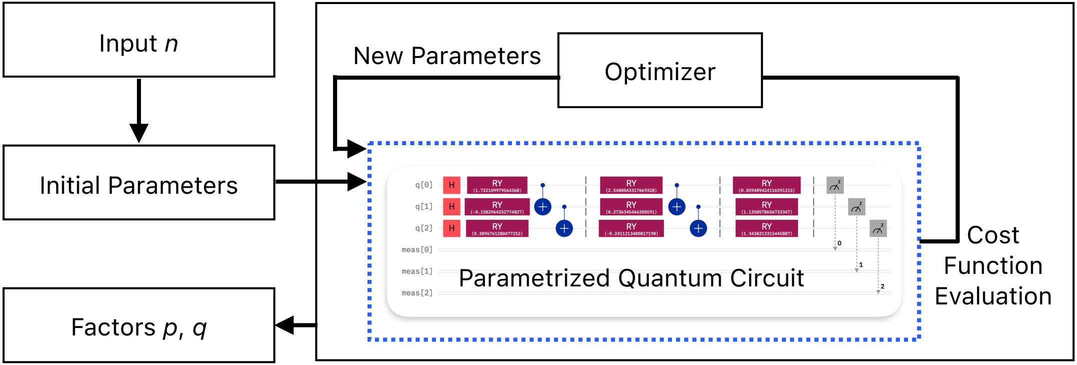
[ST16]

Project #2: Variational Factoring

- Factorize numbers using variational algorithms, primarilty VQE.
- Master-thesis by M. Sobhani, assisted by K. Jansen, T. Hartung (Northeastern Uni), E. Agathocleous (Uni Bonn),
- IBM has showed interest in this topic, perhaps it will be scaled even more.

Topics: Variational Algorithms, Encoding Schemes, Factorization, Cost Functions, Hamiltonians, Cryptography, Quantum Advantage, Mapping Optimization Problems

Project #2: Visualisation



Input *n*

Initial Parameters

Factors *p*, *q*

New Parameters

Optimizer

Cost Function Evaluation

Parametrized Quantum Circuit

Figure: Variational Factoring Visualization by Mona Sobhani.

Project #3: Attacking Elliptic-Curve Cryptography

- Bachelor’s examination with the HAW Hamburg finished in Febuary 2025.
- New resource estimates for quantum arithmetic to solve ECDLP (Elliptic Curve Discrete Logarithm Problems)
- Evaluates the current state of quantum computers for solving today’s encryption in TLS (HTTPS and SSH).

Topics: Shor’s algorithms, Discrete Logarithm Problems, Cryptography, Quantum Advantage, Paraellised Computation, Hardware optimization, Quantum Arithmetic, Encoding Schemes

Project #3: Current Trends: Qubit Count

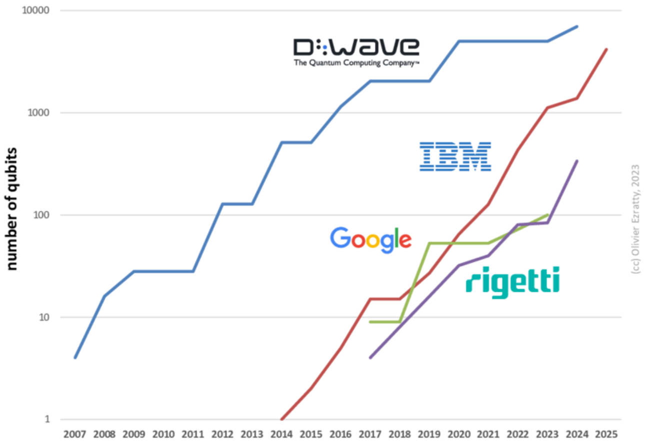


Figure: Trend for Qubit counts. [Ezr23]

Project #3: Current Trends: Quantum Volume

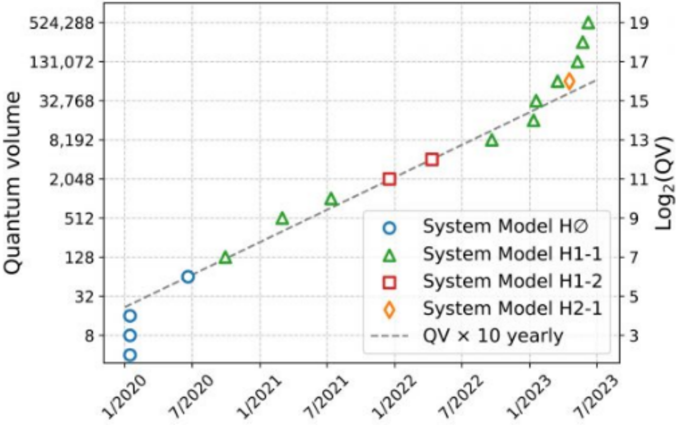


Figure: Quantinuum’s Trend for Quantum Volume. [Qua23]

Project #3: Impact

- With the current trends, perhaps IT-Security will need to be completely rethought in the end of the 2020s.
- Even ’post-quantum’ cryptography, has in some cases been proven to not be as quantum secure as intially thought, especially for isogeny based lattice-based cryptography.
- Quantum Computers importance in Big Data, Data Mining and Scientific Computing may rapidly change.

Possible QC Usecases in SC

This is not an exhaustive list!

- Usage in HEP: Lattice-Gauge theories, Parton showers / Scattering, Jet reconsutrction, Experiment simulations, Signal extraction
- Better approximations/solutions for PDEs. (Likely a downward shift in the approximatability hierarchy!)
- Usage as subroutines for specific subproblems in simulations.
- Quantum Machine Learning can have better performance in training times and quality/yield. (However, one must be careful with how exactly you are evaluating performance!)
- Parallelisation in Big Data and Data Analysis (Especially for Global attributes)
- Computational speedup for specific subproblems with global attributes.
- (Cryptographic implications)

Examples

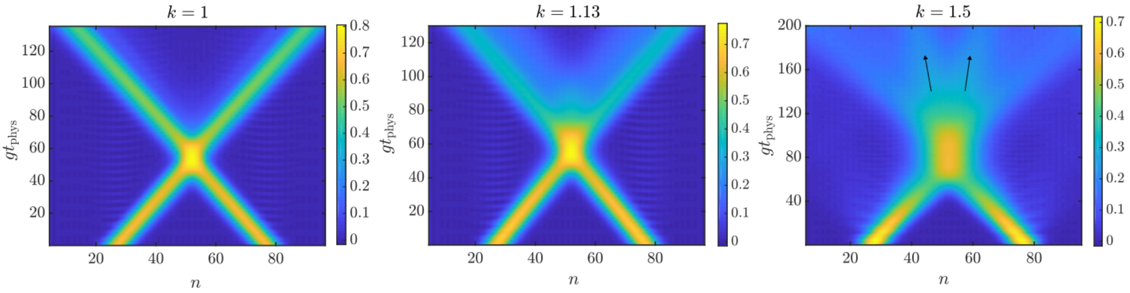
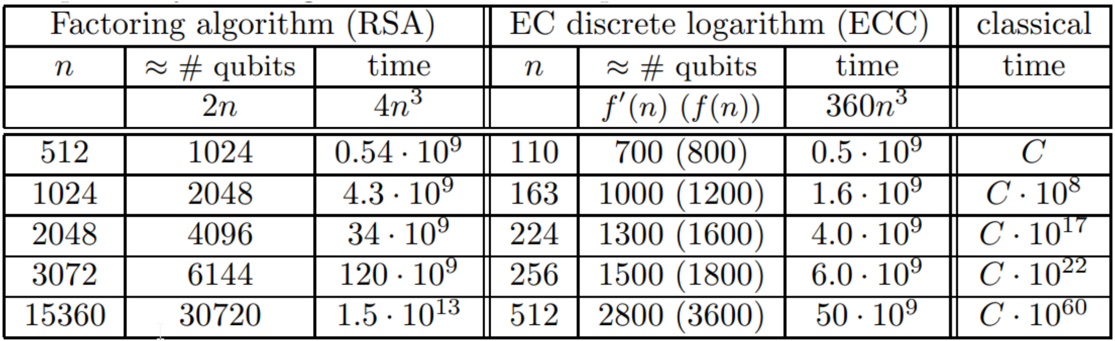


Figure: Two-site entanglement entropy to represent elastic and inelastic meson-meson scattering. [PKB24]

Examples



Factoring algorithm (RSA)			EC discrete logarithm (ECC)			classical
n	$\approx$ # qubits	time	n	$\approx$ # qubits	time	time
	$2n$	$4n^3$		$f'(n)$ $(f(n))$	$360n^3$	
512	1024	$0.54 \cdot 10^9$	110	700 (800)	$0.5 \cdot 10^9$	C
1024	2048	$4.3 \cdot 10^9$	163	1000 (1200)	$1.6 \cdot 10^9$	$C \cdot 10^8$
2048	4096	$34 \cdot 10^9$	224	1300 (1600)	$4.0 \cdot 10^9$	$C \cdot 10^{17}$
3072	6144	$120 \cdot 10^9$	256	1500 (1800)	$6.0 \cdot 10^9$	$C \cdot 10^{22}$
15360	30720	$1.5 \cdot 10^{13}$	512	2800 (3600)	$50 \cdot 10^9$	$C \cdot 10^{60}$

Figure: Resource estimates from 2003 for RSA and ECC. [PZ04]

References I

[PZ04] John Proos and Christof Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. 2004. arXiv: quant-ph/0301141 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/0301141.

[ST16] David M. South and Monica Turcato. "Review of Searches for Rare Processes and Physics Beyond the Standard Model at HERA". In: (2016). DOI: 10.1140/epjc/s10052-016-4152-3. eprint: arXiv:1605.03459.

[Ezr23] Olivier Ezratty. Is there a Moore's law for quantum computing? 2023. arXiv: 2303.15547.

[Qua23] Quantinium. Quantinuum Reports Significant Progress in Quantum Volume with H1-1 System — hpcwire.com. https://www.hpcwire.com/off-the-wire/quantinuum-reports-significant-progress-in-quantum-volume-with-h1-1-system/. [Accessed 18-06-2024]. 2023.

References II

[PKB24] Irene Papaefstathiou, Johannes Knolle, and Mari Carmen Bañuls. Real-time scattering in the lattice Schwinger model. 2024. arXiv: 2402.18429 [hep-lat]. URL: https://arxiv.org/abs/2402.18429.

Thank you!

Contact

Deutsches Elektronen-
Synchrotron DESY

www.desy.de

Lukas Mansour
iD 0009-0009-0001-8124
DESY IT & CQTA
lukas.mansour@desy.de