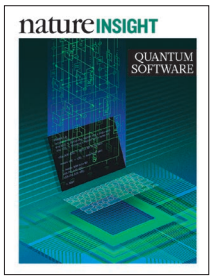
nature INSIGHT

QUANTUM SOFTWARE

14 September 2017 / Vol 549 / Issue No 7671



Cover illustration
Nik Spencer

The Campus
4 Crinan Street
London N1 9XW, UK
Tel: +44 (0) 20 7833 4000
e: nature@nature.com

SPRINGER NATURE

Decades have passed since the great minds of physics, including Richard Feynman and David Deutsch, predicted that the laws of quantum mechanics could give rise to a computing paradigm that — for certain tasks — is superior to classical computing. But controlling fragile quantum systems well enough to construct even the most primitive quantum computing hardware has proved taxing.

Experimental advances in the past few years have hushed the sceptics of quantum computing. However, the point that it is not entirely clear which application of quantum computers will redeem the hard work remains valid. This Insight discusses the applications in which quantum computers may excel and how software will actually run on such machines.

Just as programming languages and compilers facilitate interaction with the semiconductor transistors in a classical computer, many layers of software tools will sit between quantum algorithms and hardware. An important component is quantum error-correcting code. The fragility of quantum bits leads to errors during computation, and choices about how to make quantum-computing architectures fault tolerant have a knock-on effect on higher layers of the quantum tool chain.

With quantum programming languages and compilers to hand, the quantum software engineer can implement 'killer' software applications, in which the speed afforded by quantum computers will have real-world impact. Factoring using Shor's algorithm is one potential application because it could break current methods of encryption. Yet cryptographers are already devising classical cryptosystems that would guarantee security even if quantum computers achieve factoring at mesmerising speeds. Perhaps quantum machine learning will also turn out to be a killer application — it has, at least, been an important motivator for big technology companies to invest in quantum computing.

As the practical relevance of quantum computing becomes clearer, we should not forget the part that foundational thinking played in its inception. Research on the fundamental limits of classical versus quantum computing remains fascinating — and may even help to surmount quantum engineering hurdles.

Leonie Mueck
Senior Editor

CONTENTS

REVIEWS