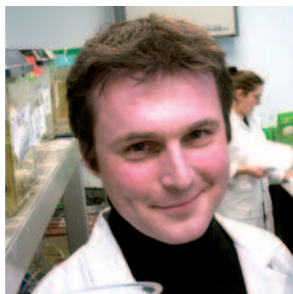
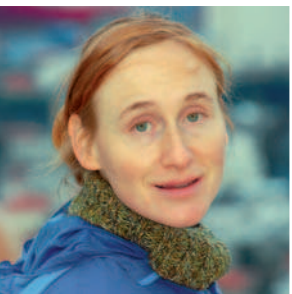


The **ERC** Starting Grant

Supporting the next generation of research leaders in Europe



European Research Council



Preparing for tomorrow's computers

Quantum computing promises to add subtle grey shades to the black-and-white logic of today's digital computers, replacing the binary strings of '0's and '1's now used to encode data with the unit of quantum information known as a 'qubit'. Starting Grant recipient Julia Kempe, a highly qualified international researcher now working in Israel, will bring a similarly sophisticated mix of physics and mathematics to the study of phenomena that will provide unprecedented problem-solving powers to the IT tools of the future.



Born in East Berlin, Julia Kempe has always been consumed by a thirst for knowledge. 'Even as a very young child, I was constantly asking my parents to give me riddles and puzzles to solve,' she recalls. This natural curiosity remains as strong today, driving her to pursue a career path of intense study and achievement that has marked her out as one of Europe's outstanding young researchers – and a worthy recipient of the ERC Starting Grant.

Road to IT revolution

Her chosen field, quantum computing, has the potential to revolutionise information technology. Today's digital computers store and manipulate 'bits' of data, which can be considered as strings of on/off signals or '0's and '1's. In contrast, a quantum computer would obey the laws of quantum physics, which take over from classical physics at the atomic scale of matter. Here, the fundamental unit of information (the qubit) can exist not only as a 0 or 1, but also as a blend or superposition of the two, when it behaves as if it were in both states simultaneously.

This curious phenomenon holds the key to a massive boost in the power of computers to solve problems that are beyond present capabilities. It has been the subject of international research interest since Peter Shor's breakthrough announcement in 1994 of an algorithm making it possible to derive the prime factors of very large numbers within an acceptable time-frame – something that cannot be achieved with classical computers.

Shor's discovery is not just of academic interest; it could, for example, show the way to defeat the cryptographic systems currently employed to safeguard online financial transactions and secure sensitive databases.

Early promise fulfilled

Julia's progress into this esoteric world began in her early years, when she was soon earmarked for a place at a school for gifted pupils. In this stimulating environment, she learned problem-solving skills that helped her to win several national prizes in mathematics and science.

Shortly after the fall of the Berlin wall in 1989, the Kempe family left East Germany for Austria, where Julia gained degrees in both maths and physics at the University of Vienna. During this time, an exchange visit to Sydney's University of Technology fired her interest in discovering new locations and acquiring new experiences.

Her next move was to France, where she mastered in algebra at the Pierre and Marie Curie University, Paris, and in theoretical physics at the city's École Normale Supérieure. Armed with an impressive array of qualifications at the age of only 23, she went on to accept the gruelling demands of simultaneous PhD programmes in quantum computing – one in Paris, the other at Berkeley University, California!

This remarkable record led to the early offer of a position as permanent researcher at the *Centre Nationale de Recherche Scientifique* (CNRS),

“ Having operated more or less independently throughout my career to date, the EU funding will enable me to build a group of students and pass on some of my passion for crossing traditional boundaries. ”

France, where the liberal rules gave her the freedom to spend more time pursuing post-graduate studies at Berkeley and elsewhere.

In 2006, Julia won a CNRS bronze medal and the Prix Joliot-Curie as France's outstanding young female researcher of the year. She was also awarded an Alon Fellowship by the Higher Council for Academic Studies in Israel, which provided basic support for a three-year tenure at Tel Aviv University.

'I applied for a Starting Grant after learning about them from the university's funding department. Naturally, I was very happy to hear that my proposal had been accepted,' she says. 'Having operated more or less independently throughout my career to date, the EU funding will enable me to build a group of students and pass on some of my passion for crossing traditional boundaries.'

'It is fortunate that the provisions of the ERC scheme are such that I could qualify while working in an Associate Country. I am obviously a firm believer in researcher mobility, and am actively collaborating with quantum computing groups around the world.'

New research direction

Julia's plans for the QUCO project straddle the divide between algorithm design, cryptography, complexity and physics. The overarching idea is not only to explore the power of quantum machines, but also to identify their limits. 'We do not yet know what form a quantum computer would

actually take,' she points out. 'It could be a decade or more away, but meanwhile there are many fascinating avenues for theoretical investigation.'

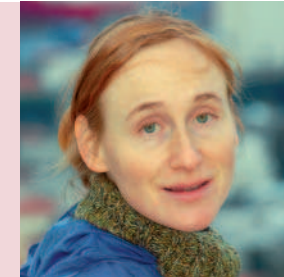
'So far, most research has addressed areas where quantum computers are much faster, or otherwise better, than classical computers. We propose to turn this around and look for problems that remain hard even for a quantum computer — and which might form the basis of new, secure cryptosystems. Information is a crucial commodity to the economy and society at large. It must be protected not only against current computational challenges, but also against future quantum-equipped attackers.'

A second aim is to ascertain the power of quantum resources, such as entanglement (the sharing of a quantum state between two parties) and its effects in quantum communication. Quantum memory is another resource that could become available long before a functional quantum computer is built. 'In this context, we again propose to focus on a cryptographic theme, namely how current classical cryptographic schemes could be compromised if an adversary has quantum memory at his disposal. We would also like to further explore the computational power of quantum machines and quantum physical systems in complexity theory terms, comparing them with their classical counterparts.'

Thirdly, an interesting trend in quantum computation is the 'reverse' flow of techniques and results, using the quantum information toolbox to answer classical questions. 'Many theoretical findings from

the quantum world could no doubt be exploited in the classical arena,' Julia maintains. 'We propose to explore the connections in algorithm design and learning theory, and to initiate a systematic way to obtain classical results the 'quantum' way.'

'The Starting Grant will allow me to hire postdoc, PhD and master's students to share in this exciting project, as well as inviting visitors and providing for material and travel costs on a scale appropriate to a leading research team.'



Principal Investigator
Julia Kempe

Nationality, age
German, 34

Project title
The Power of Quantum Computers

Acronym
QUCO

Host Institution
Tel Aviv University
School of Computer Science
Schreiber 121
69978, Tel Aviv, Israel

Grant
EUR 744 000

Project duration
60 months

Further information
kempe@post.tau.ac.il
www.cs.tau.ac.il/~kempe/