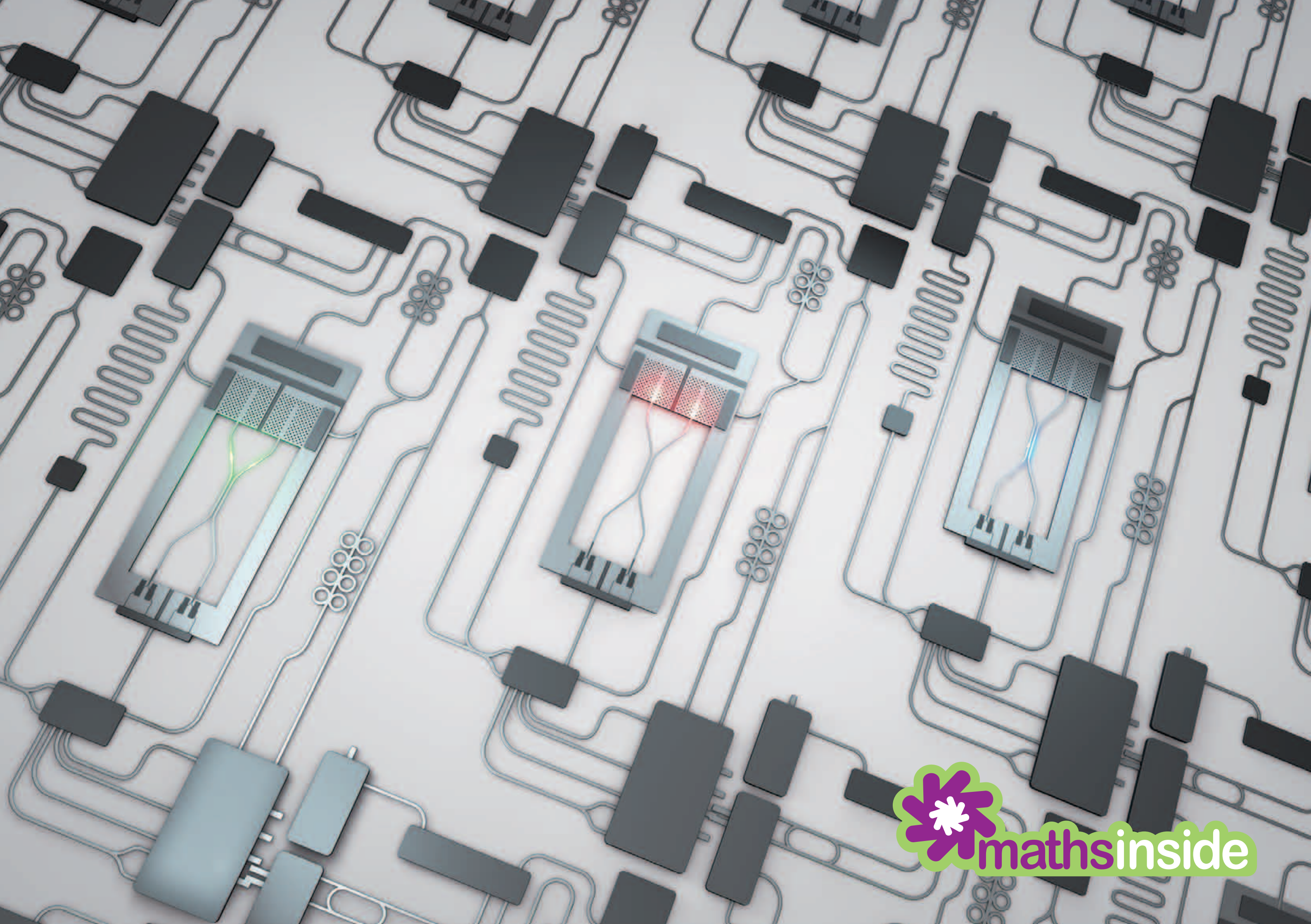
mathsinside

QUANTUM COMPUTING

Cracking codes with the help of mathematics

Cracking Cryptography with Quantum Computers

Researchers at the University of Sheffield are building an integrated optical circuit that could be part of the processor for a quantum computer. Quantum computers are different from ordinary computers, they exploit quantum mechanics to perform calculations in entirely new ways. This difference makes quantum computers particularly good at cracking codes commonly used in cryptography.

What is Cryptography?

Cryptography is the study of secret codes: disguising information so that no one but the intended reader can understand it. It's not just used by spies though – every time you buy something online your computer encrypts your payment information so that if anyone intercepts your messages they cannot steal your credit card!

Prime Factorisation

Computer cryptography uses prime numbers: numbers that are divisible only by 1 and themselves, *eg* 3, 5 and 7 are primes while 6, 9 and 14 are not. Any number can be written as the product of certain prime numbers multiplied together, *eg* 30 = 2 x 3 x 5.

Computer cryptography relies on the fact that for very large numbers, with 200 digits say, this prime factorisation is very hard to find, especially if the number is the product of just two very large prime numbers. This means that you can share the product of two large prime number with others over the internet and they won't know the two numbers you started with. The part you share is called your public key, while the two numbers you started with are called your private key. Using your public key, others can encrypt information so that only you (using your private key) can read it. A normal computer would need tens of thousand of years to find someone's private key from their public key of 200 digits!

The length of time a computer takes to factorise a number into primes largely depends on how large the number is – the bigger the number the longer it takes. Some algorithms – the set of instructions the computer performs – are better than others and take less time than others. The best factorisation algorithm so that an ordinary computer can run works in exponential time. This means that the time needed grows exponentially with the length of the input: roughly, if x is the number of digits in the number then the required time grows like 2^x. This gets very big very quickly and makes running the algorithm for large numbers essentially impossible.

Quantum computers, however, can use a far better algorithm, called Shor's algorithm. Using this algorithm the time required only grows polynomially, roughly like x^2. So for very long numbers a quantum computer can vastly outperform an ordinary one. For examples of the times required using ordinary and quantum computers visit **www.ldsd.group.shef.ac.uk/ql/**

The University Of Sheffield.

LONDON MATHEMATICAL SOCIETY 150 YEARS

Institute of mathematics & its applications

selected THE ROYAL SOCIETY SUMMER SCIENCE EXHIBITION 2015

mathsinside

Design: www.blitzbranding.co.uk cover image: www.23i.co.uk