Quantum Computing and Cryptography

Cryptography

School of Engineering and Technology
CQUniversity Australia

Prepared by Steven Gordon on 04 Jan 2022,
quantum.tex, r1971

Contents

Quantum Computing

Quantum Algorithms

Issues in Quantum Computing

Quantum Cryptography

Cryptography in the Quantum Era

Quantum Technology (definition)

Emerging technologies that build upon concepts of quantum physics, especially superposition and entanglement. Includes quantum computing and quantum cryptography.

bit (definition)

Binary digit, 0 or 1, as the basic unit of information in classical computers. For example stored as electric charges in capacities or with magnets in hard disks. Communicated with electrical or optical pulses. A bit has two states: 0 or 1.

qubit (definition)

Quantum bit has states represented in a quantum-mechanical system. The state of a qubit is a vector. A qubit has two *basis states*, $|0\rangle$ and $|1\rangle$, but many possible states in between. Often represented using subatomic particles such as electrons or photons.

Quantum Superposition (definition)

Any two (or more) quantum states can be added together to form another quantum state. That result is a superposition of the original states.

qubit Superposition (example)

Basis state $|0\rangle$ is like bit 0. Basis state $|1\rangle$ is like bit 1. The state $0.6|0\rangle + 0.8|1\rangle$ is an example of a superposition of the two basis states, and forms another state of the qubit. Another example state is $0.866|0\rangle + 0.5|1\rangle$. In general, a superposition state is $\alpha|0\rangle + \beta|1\rangle$, where $\alpha^2 + \beta^2 = 1$.

The Measurement Problem (definition)

Measuring a qubit gives the bit 0 with probability α^2 and bit 1 with probability β^2. After measurement the qubit enters (collapses into) the basis state.

Quantum Entanglement (definition)

Pair of particles are dependent on each other, meaning the quantum state of one particle impacts on the other.

qubit Entanglement (example)

If 2 qubits are entangled, then if one qubit is measured to be 0, then the other qubit will also be measured to be 0 (and similar if measured as 1).

Quantum Computation (informal) (definition)

A quantum computation starts with a set of qubits, modifies their states to perform some intended calculation, and then measures the result.

Classical Computer Circuits (definition)

Circuits in classical computers are built from logic gates, such as AND, NOT, OR, XOR, NAND and NOR.

Quantum Computer Circuits (definition)

Circuits in quantum computers are built from quantum logic gates. Single-bit gates include NOT, Hadamard, Phase and Shift gates; two-bit gates include Controlled NOT and SWAP; as well as 3-qubit Toffoli and Fredkin gates. Not all quantum gates have analagous operation with classical gates.

Quantum Computer (definition)

A (digital) quantum computer is built from a set of quantum logic gates, i.e. quantum circuits, and is said to perform quantum computation on qubits. An analog quantum computer also operates on qubits, but rather than using logic gates, using concepts of quantum simulation and quantum annealing.

Contents

Quantum Computing

Quantum Algorithms

Issues in Quantum Computing

Quantum Cryptography

Cryptography in the Quantum Era

Quantum Register (definition)

A quantum register is a set of *n* qubits. With a classical 2-bit register, there are four possible states: 00, 01, 10 and 11. A quantum 2-bit register can be in all four states at one time, as it is a superposition of the four states: $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$. Measuring the register will return one of the four states, with probability depending on the weights.

Quantum Parallelism (definition)

Consider a circuit that takes x as input and returns $f(x)$ as output. Normally, passing in an input, sees the function applied once, and one output produced. Using quantum gates, such as a Fredkin gate, if x is a quantum register with a superposition of states, it is passed as input and the function is applied once. But the function operates on all of the states of the quantum register, returning output that contains information about the function applied to all states.

Classical Function (example)

Consider the function $f(x) = 3x \bmod 8$. Assume we want to calculate all possible answers for $x = 0, 1, 2, \ldots, 7$. With a classical computer we would have a 3-bit input to a circuit that calculates $f(x)$, i.e. performs the modular multiplication. To find all possible answers we would calculate $f(0) = 0$, $f(1) = 3$, $f(2) = 6$, $f(3) = 1$, $f(4) = 4$, $f(5) = 7$, $f(6) = 2$, and $f(7) = 5$. The function/circuit is applied 8 times.

Quantum Function (example)

Now consider the same function, $f(x) = 3x \bmod 8$, but implemented with a quantum circuit. We initialise a quantum register with 3 qubits. This register is in a superposition of 8 states at once: 000, 001, 010, 011, 100, 101, 110 and 111. The quantum register is input to the circuit. The output register will have 3 qubits in a superposition that contains *all 8 answers*. By applying the function/circuit only once, we obtain an output that has information about all 8 answers. This represents a speedup of a factor of 8 compared to the classical example!

Quantum Algorithm (definition)

A quantum algorithms are usually a combination of classical algorithms/computations and quantum computations. First pre-processing is performed using classical techniques. Then the input quantum register is prepared, a quantum calculation performed, and output quantum register is measured. There may be some post-processing of the result with classical techniques. If the result is as desired, then exit, otherwise repeat the process. Repetition is usually needed due to both errors in quantum calculations and the probabilistic nature of the result.

Grover's Search Algorithm (definition)

Consider a database of N unstructured data items (e.g. not sortable). Search is performed by applying a boolean function on input that returns true if correct answer. Classical search takes $\mathcal{O}(N)$ applications of function. Grover's quantum search algorithm takes $\mathcal{O}(\sqrt{N})$ applications of function.

Worst Case Brute Force Attempts with Classical and Quantum Algorithms

Key length [bits]	Classical	Quantum
64	2^{64}	$\sqrt{2^{64}} = 2^{32}$
128	2^{128}	$\sqrt{2^{128}} = 2^{64}$
256	2^{256}	$\sqrt{2^{256}} = 2^{128}$
512	2^{512}	$\sqrt{2^{512}} = 2^{256}$

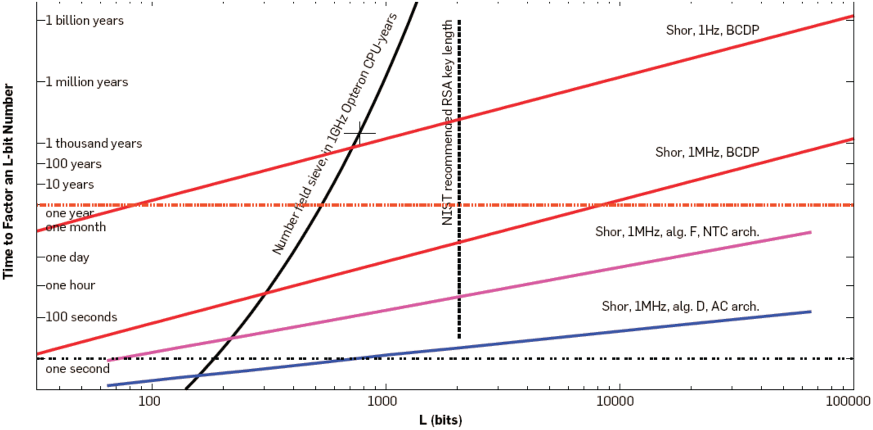
Integer Factorisation with General Number Field Sieve (definition)

Given an integer N, find its prime factors. A general number field sieve on classical computer takes subexponential time, about $2^{\mathcal{O}(N^{1/3})}$.

Integer Factorisation with Schor's Algorithm (definition)

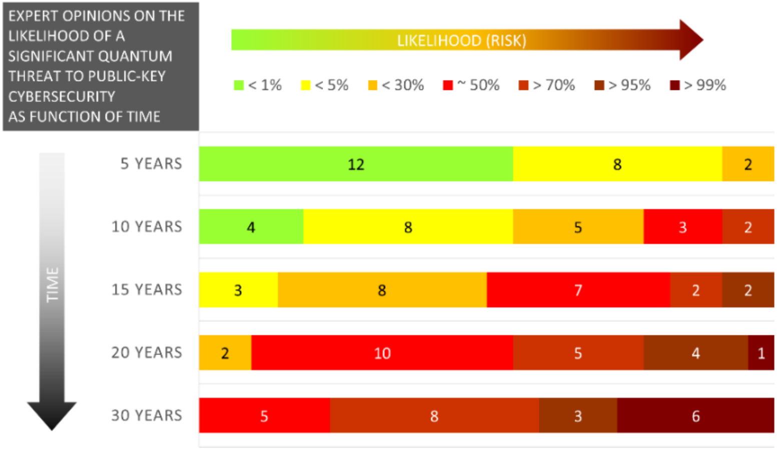
Given an integer N, find its prime factors. Shor's algorithm on a quantum computer takes polynominal time, about $\log N$.

Scaling the classical number field sieve (NFS) vs. Shor's quantum algorithm for factoring



Credit: Figure 1 from A Blueprint For Building a Quantum Computer by Van Meter and Horsman, Communications of the ACM, Oct 2013. Copyright by Van Meter and Horsman and ACM.

Likelihood quantum computers significant threat to public-key cryptosystems



Numbers reflect how many experts (out of 22) assigned a certain probability range.

Credit: Quantum Threat Timeline Report, Michele Mosca and Marco Piani, from evolutionQ and the Global Risk Institute, 2019.

Contents

Quantum Computing

Quantum Algorithms

Issues in Quantum Computing

Quantum Cryptography

Cryptography in the Quantum Era

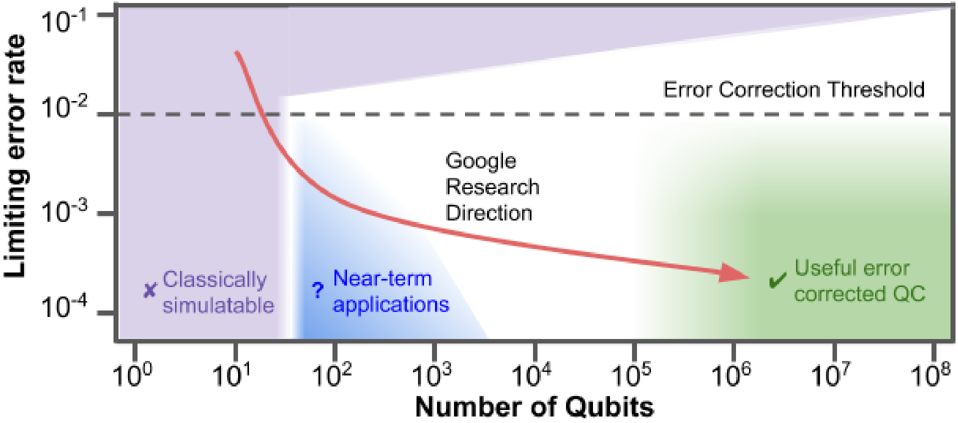
Decoherence in Quantum Computing (definition)

In their coherent state, qubits are described as a superposition of states. The loss of coherence (i.e. decoherence) means the qubits revert to their "classical" basis states. They no longer exhibit the unique quantum properties. Decoherence times vary for different system; for example IBM quantum computers about 100 μs.

Errors in Quantum Computing (definition)

Errors frequently occur due to various reasons including: decay of individual qubits; environmental defects that impact multiple qubits; interference between qubits and other systems; accidental measurement of qubits; and even loss of qubits. Significant research effort is on designing error correcting schemes.

Quantum error rates vs qubits and intended direction of Google Quantum Research



Credit: Google Research, A Preview of Bristlecone, Google's New Quantum Processor

Cooling (definition)

For qubits to maintain coherence, quantum circuits need to be very cold, approaching 0 Kelvin or -273 C.

Quantum Computers in Practice

- For more detailed comparison see the Quantum Computing Report
- Google: Sycamore 53-qubit (2019)
- IBM: 5- and 16-qubit machines available for free; 20-qubit machine available via cloud; 53-qubit machine (2019)
- Rigetti: Aspen-7 28-qubits (2019)
- D-Wave systems: 2000Q has 2048-qubits, however using different technology (quantum annealing) that cannot be used to solve Shor's algorithm

Contents

Quantum Computing

Quantum Algorithms

Issues in Quantum Computing

Quantum Cryptography

Cryptography in the Quantum Era

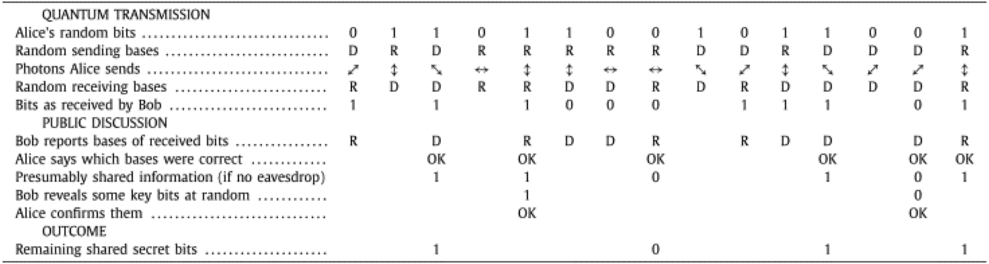
Quantum Cryptography (definition)

Quantum cryptography refers to techniques that apply principles of quantum systems to build cryptographic mechanisms. The most widely technique is quantum key distribution. Others approaches often involve agreements between parties that do not trust each other.

Quantum Key Distribution (informal) (definition)

The aim of QKD is for two parties to exchange a secret key (similar to DHKE). A chooses random bits, as well as corresponding random modification of states (called *sending basis*). Applied together using a fixed scheme, A generates and sends photons in quantum states. B chooses own random *measuring basis* and measures the photons. A then informs B their sending basis, and allowing B to recognise which of the measured photons to consider (i.e. those where the measuring basis and sending basis match). B uses the resulting bits as a secret key, however only after confirming with A that there are no errors in the key (e.g. sending a challenge encrypted with the key).

Example of BB84 Quantum Key Distribution



QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Credit: Bennett and Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical Computer Science, Dec 2014, Copyright Elsevier.

QKD security (informal) (definition)

An attacker C tries to learn the secret key between A and B, without A or B knowing. Therefore the attacker has to measure the photons sent by A. However, as the photons are a superposition of states, when C measures them, they are changed. As a result, B will receive changed photons, and when they check the secret key with A, the check will fail.

Contents

Quantum Computing

Quantum Algorithms

Issues in Quantum Computing

Quantum Cryptography

Cryptography in the Quantum Era

Post-Quantum Cryptography

- NIST Post-Quantum Cryptography project called for proposals on quantum-resistant public key cryptography algorithms
  - Digital signatures, public-key encryption, key exchange
  - 69 submissions in round 1 (2017)
  - 26 algorithms in round 2 (2019)
  - 7 finalists in round 3 (2020)
  - Plan to standardise in 2022/2023
- Open Quantum Safe has open-source software for prototyping quantum-resistant cryptography, including forks of OpenSSL, OpenSSH and OpenVPN