Glossary

active optical switch

An optical switch is a multi-port network bridge, which connects multiple optic fibres to each other and controls data packets routing between inputs and outputs. An active optical switch has optical gain elements.

adiabatic theorem

The adiabatic theorem is a concept in quantum mechanics. Its original form, due to the German-British physicist and mathematician Max Born and the Russian physicist Vladimir Fock, was stated as follows: “A physical system remains in its instantaneous eigenstate if a given perturbation is acting on it slowly enough and if there is a gap between the eigenvalue and the rest of the Hamiltonian's spectrum”.

In simpler terms: a quantum mechanical system subjected to gradually changing external conditions adapts its functional form, but when subjected to rapidly varying conditions there is insufficient time for the functional form to adapt, so the spatial probability density remains unchanged.

Adiabatic Quantum Computing (AQC)

Adiabatic Quantum Computing (AQC) is a form of quantum computing which relies on the adiabatic theorem to perform calculations and is closely related to quantum annealing.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a variant of the Rijndael block cipher developed by the Belgian cryptographers Joan Daemen and Vincent Rijmen. Rijndael is a symmetric-key cryptographic algorithm and consists of a family of ciphers with different key and block sizes.

AES is included in the ISO/IEC 18033-3 standard and has been adopted by the US government; it supersedes the Data Encryption Standard (DES). For AES, NIST FIPS 197 specifies three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

amplitude

This term has various meanings depending on the context. It can be the classical amplitude of a wave, i.e. half of its maximal variation, as opposed to its phase. For a quantum object, it can be the complex amplitudes of its basis states or eigenvectors. With a qubit in its Bloch sphere representation, the amplitude is related to the projection of the qubit vector on the z axis. But the α and β describing the qubit vector $\alpha|0\rangle + \beta|1\rangle$ are also amplitudes (although complex amplitudes, which define the qubit's probability amplitudes and its relative phase).

ancilla qubit

The meaning of “ancilla” in ancilla qubit is “auxiliary”. Ancilla qubits are for example used in Quantum Error Correction (QEC) to determine the error syndrome.

annealing

In metallurgy and materials science, annealing is a heat treatment that alters the physical and sometimes chemical properties of a material to increase its ductility and reduce its hardness, making it more workable. It involves heating a material above its recrystallisation temperature, maintaining a suitable temperature for an appropriate amount of time and then cooling.

anyon

Quasiparticles inhabit so-called quasi-worlds, which were invented to enable the understanding of the properties of exotic materials and exotic states of matter. An anyon is a quasiparticle in a 2-dimensional space. Anyons are neither fermions nor bosons (both of which are particles in a 3-dimensional space): they have statistical properties intermediate between fermions and bosons.

The term anyon was introduced by the American theoretical physicist Frank Anthony Wilczek.

atom

An atom is the smallest unit of matter ("atom" is Greek for “indivisible”) that forms a chemical element, i.e. a substance whose atoms are all of the same kind. Atoms are composed of a nucleus (Latin for “kernel”) and one or more electrons in probabilistic locations around the nucleus (so-called “orbitals”).

The atom's nucleus contains one or more protons and one or more neutrons, except for hydrogen-1 (the lightest element) which has only one proton and no neutrons in the nucleus of its atoms. The number of protons in the nucleus is the so-called atomic number, which is the defining property of an element. Elements are arranged by their atomic number in the Periodic Table of Elements.

The mass number of an element is the sum of the protons and neutrons in the nucleus of its atoms. The heaviest known element is uranium-238, with 92 protons and 146 neutrons. Elements with the same number of protons but different numbers of neutrons in the nucleus of their atoms are called isotopes.

Protons and neutrons behave similarly within an atom's nucleus and both have a mass of approximately one atomic mass unit (which is more than 2,000 times the mass of an electron) hence they are collectively referred to as nucleons. Whereas electrons are elementary subatomic particles, nucleons are made up of elementary subatomic particles called quarks, which are the smallest known units of matter.

Neutrons have no electric charge, protons have a positive electric charge and electrons have a negative electric charge. If the number of protons and electrons in an atom balance, it is electrically neutral (a neutral atom). If an atom has more or fewer electrons than protons, it has an overall negative or positive electric charge and is called an ion. On earth and on other planets most of the matter is in the form of (neutral) atoms, but in the sun and other stars most of the matter is in the form of ions (hence most of the matter in the universe is probably in the form of ions).

Backus-Naur Form (BNF)

Backus–Naur Form (BNF) is a meta-syntax notation for context-free grammars used to describe the syntax of computer programming languages, document formats, instruction sets and communication protocols. BNF was developed by the American computer scientist John Warner Backus and the Danish computer scientist Peter Naur.

Many extensions and variants of the original BNF notation are in common use, some of which are exactly defined, including Extended Backus–Naur Form (EBNF) and Augmented Backus–Naur Form (ABNF).

beam splitter

A beam splitter is an optical device that splits a beam of light in two. It is usually made with two glued triangular glass prisms. Polarising beam splitters are a particular class of beam splitters that use birefringent materials to split light into two beams of orthogonal polarisation states.

Bell inequality testing

In 1964, in response to the Einstein-Podolsky-Rosen (EPR) paradox formulated in 1935 by the Swiss-American theoretical physicist Albert Einstein 1935, the Russian-American physicist Boris Yakovlevich Podolsky and the American-Israeli physicist Nathan Rosen, an analysis of quantum entanglement was carried out by the Northen Ireland physicist John Stewart Bell. He deduced that if measurements are performed independently on the two separated halves of a pair of entangled particles, then the assumption that the outcomes depend upon 'local hidden-variables' within each half implies a constraint on how the outcomes on the two halves are correlated. This constraint would later be named the 'Bell inequality'.

Quantum mechanics predicts correlations that violate this inequality and multiple variations on Bell's theorem have been tested experimentally in physics laboratories many times. All these 'Bell tests' have found that the hypothesis of 'local hidden-variables' is inconsistent with the way that quantum entanglement works. While the significance of Bell's theorem is not in doubt, its full implications for the interpretation of quantum mechanics remain unresolved.

Bell's theorem

Bell's theorem is used to prove that quantum mechanics is incompatible with 'local hidden-variable' theories. It was introduced by the Northen Ireland physicist John Stewart Bell in a 1964 in response to the Einstein-Podolsky-Rosen (EPR) paradox. The EPR paradox refers to a thought experiment formulated in 1935 by the Swiss-American theoretical physicist Albert Einstein 1935, the Russian-American physicist Boris Yakovlevich Podolsky and the American-Israeli physicist Nathan Rosen, in order to argue that quantum mechanics was an incomplete theory. In this view (shared by many other leading physicists at the time), quantum particles carry physical attributes (later called 'local hidden-variables') which are not included in the quantum mechanics theory, and the uncertainties in quantum mechanics theory's predictions are due to ignorance of these attributes.

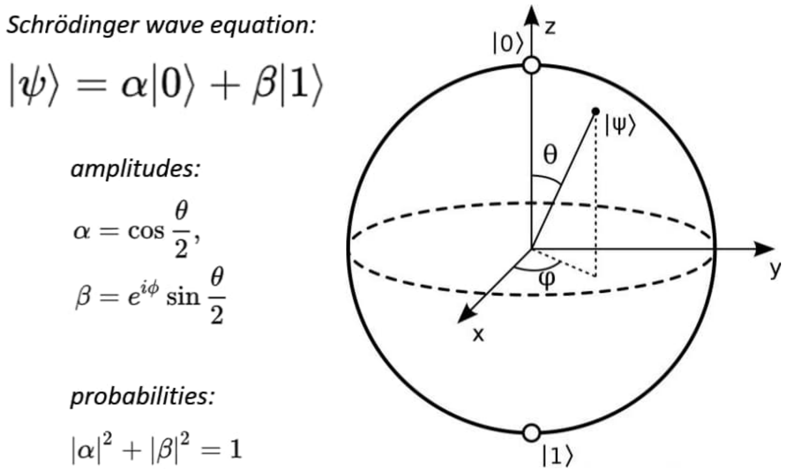
Blind Quantum Computation (BQC)

Homomorphic encryption is a technique that allows users to encrypt their data at their own site before sending it for processing to a cloud service. The cloud service executes a program while the data is still encrypted and then sends the encrypted results back to the users, which can then decrypt the results. The cloud service provider would not be able to determine the input data or the output data because the data is encrypted by the cloud service users but access to the program that was executed by the cloud service could still be a potential security issue.

Blind Quantum Computation (BQC) goes a step further in that it cannot only hide the input and output data, but also the program executed by a cloud-based quantum computer. It does require a quantum internet connection to the cloud service, but potentially this approach can provide the same level of security and privacy as having the quantum computer on-premise.

Bloch sphere

The Bloch sphere (named after the Swiss-American physicist Felix Bloch) is a geometrical representation of the pure quantum state space of a two-level quantum mechanical system, e.g. a qubit. The Bloch sphere has antipodal points corresponding to a pair of mutually orthogonal quantum state vectors. The north and south poles of the Bloch sphere correspond to the standard basis vectors |0⟩ and |1⟩ of the qubit.


Schrödinger wave equation:
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
amplitudes:
$\alpha = \cos\frac{\theta}{2},$
$\beta = e^{i\phi}\sin\frac{\theta}{2}$
probabilities:
$|\alpha|^2 + |\beta|^2 = 1$
|0⟩
z
|ψ⟩
θ
φ
y
x
|1⟩

The qubit quantum state can also be represented as:

$|\Psi\rangle = r_{\alpha}e^{i\phi_{\alpha}}|0\rangle + r_{\beta}e^{i\phi_{\beta}}|1\rangle$

or $|\Psi\rangle = e^{i\phi_{\alpha}}(r_{\alpha}|0\rangle + r_{\beta}e^{i(\phi_{\beta} - \phi_{\alpha})}|1\rangle)$

The *global phase* $e^{i\phi_{\alpha}}$ has no significance[1], therefore:

$|\Psi\rangle = r_{\alpha}|0\rangle + r_{\beta}e^{i(\phi_{\beta} - \phi_{\alpha})}|1\rangle$

[1] The probabilities of the various measurement outcomes are exactly the same when we measure |0⟩ or when we measure $e^{i\phi_{\alpha}}|0\rangle$; because of this we say that the “global phase” $e^{i\phi_{\alpha}}$ has no physical significance.

The *relative phase* ϕ_β - ϕ_α is then replaced with ϕ (0 .. 2π radius); therefore:

$|\Psi\rangle = r_\alpha|0\rangle + r_\beta e^{i\phi}|1\rangle$ where $r_\alpha = \cos(\theta/2)$, $r_\beta = \sin(\theta/2)$ with $0 \leq \theta \leq \pi$.

α and β are probability amplitudes ($|\alpha|^2+|\beta|^2 = 1$) and θ and ϕ are angles on the Bloch sphere.

Boolean algebra

Boolean algebra, developed by the British mathematician, philosopher and logician George Boole, makes it possible to treat certain parts of logic algebraically. A Boolean value is a binary digit (bit) that can take on one of two values. These two values are usually represented by “true” and “false” in Boolean algebra, but can also be represented by something else, in particular “0” and “1”. The three basic operations in Boolean algebra, which allow us to express any Boolean function whatsoever, are the *not*, *and* and *or* binary operations.

Born rule

According to the Born rule, in a superposition of quantum states the squared norm of the amplitude of a quantum state is the probability of that quantum state resulting after measurement. Furthermore, the sum of these probabilities equals 1. Example: the superposition state $|\Psi\rangle$ of the basis states $|0\rangle$ and $|1\rangle$ of a qubit is denoted as follows:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

The probability amplitudes α and β of the qubit’s basis states are complex numbers and the squares of their norms add up to 1:

$$|\alpha|^2 + |\beta|^2 = 1$$

The vertical bars | and | denote the norm (aka modulus). The norm $|z|$ of a complex number z = a + bi is the length of the vector from the origin to the point (a, b) in a two-dimensional plane. According to the Pythagorean theorem:

$$|z| = \sqrt{a^2 + b^2}$$

The Born rule is named after the German-British physicist and mathematician Max Born.

boson

There are two fundamental classes of subatomic particles: bosons and fermions. A boson is a subatomic particle whose spin quantum number is an integer value (0 , 1 , 2 , 3 , etc.). There are two types of bosons: elementary bosons and non-elementary bosons. Elementary bosons are elementary subatomic particles. Some elementary bosons, e.g. the photon (associated with the electromagnetic force), the gluons (associated with the strong force) and the W and Z bosons (associated with the weak force), give rise to forces between other particles. One elementary boson, the Higgs boson (with spin 0), named after the British theoretical physicist Peter Ware Higgs, gives rise to the phenomenon of mass (all of space is assumed to be filled with a Higgs field, a background of virtual Higgs bosons that pop in and out of existence). The Higgs boson is different from the other elementary bosons (photon, gluons, W and Z bosons) in that it doesn't involve anything resembling a force.

Non-elementary bosons, e.g. mesons and stable nuclei of even mass number (such as hydrogen-2 and helium-4), are composite subatomic particles made up of smaller constituents.

Unlike fermions, bosons are not subject to the Pauli exclusion principle and they can thus occupy the same place at the same time. For example, in a laser beam many photons occupy the same quantum state with the same colour, the same direction and the same spatial profiles. Other well-known examples of bosonic behaviour are superconductivity and superfluidity, where large number sf Cooper pairs of electrons or helium-4 atoms, respectively, occupy the same quantum state and thus flow coherently[2].

The name boson is in honour of Satyendra Nath Bose, an Indian physicist who developed a quantum theory for these particles together with the Swiss-American theoretical physicist Albert Einstein (known as the Bose-Einstein statistics).

bra-ket notation

The bra-ket notation (aka Dirac notation) is used to denote quantum states. The notation uses the angle brackets ⟨ and ⟩ and the vertical bar | to construct "bras" and "kets". It is so called because the inner product (aka dot product or scalar product) of two quantum state vectors is denoted by ⟨Φ | ψ⟩, consisting of a left part ⟨Φ| called the bra, and a right part |ψ⟩ called the ket. Bra–ket notation was created by British theoretical physicist Paul Adrien Maurice Dirac.

[2] In simple words: in contrast to fermions, bosonic ensembles are natural conformists and prefer to be in the same state. At very low temperatures, they are less distracted by the external world and get to do what they want to do, which ns to do the same thing.

bullshit versus horseshit

There is a major difference between both: “bullshit” implies deception while “horseshit” stems from ignorance.

According to Hanlon’s razor: “never attribute to malice that which is adequately explained by stupidity” (Robert. J. Hanlon).

“Bullshit” is a serious accusation and should be substantiated as the claimant puts himself or herself in a vulnerable position: if you fight shit, you are going to end up covered in it.

calibration

Calibration is a technique to reduce systematic errors in quantum circuits. Qubit calibration is required for certain qubit technologies (e.g. superconducting qubits) due to variations in the qubit manufacturing process.

cat qubit

Cat qubits are based on microwave cavities, using two coherent states of microwaves of the same amplitude and opposite phase as the qubit’s basis quantum states. The cavities are connected to a transmon qubit that is used only for their preparation, readout and/or correction.

cavity-spin qubit

Cavity-spin qubits are based on the control of electron spins tapped in artificial defects of crystalline structures (e.g. artificial diamonds, carborundum, etc.), in which one atom in the crystalline structure is replaced by another atom and another atom is replaced by a gap (aka cavity).

CCNOT gate

A CCNOT (Controlled CNOT) gate (aka C2NOT gate or Toffoli gate) is a quantum gate operating on three qubits which modifies the value of the third qubit if the quantum state of the first two qubits is $|1\rangle$.

Chosen Ciphertext Attack (CCA)

A Chosen-Ciphertext Attack (CCA) is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

Church-Turing Thesis (CTT)

According to the Church-Turing Thesis (CTT), named after the British mathematician Alan Turing and the American mathematician Alonzo Church, if an algorithm can be performed on any piece of hardware, there is an equivalent algorithm for a Universal Turing Machine (UTM). There are also variants of the CTT:

- Strong Church-Turing Thesis (SCTT): any algorithm can be simulated efficiently using a UTM;
- Extended Church-Turing Thesis (ECTT): any algorithm can be simulated efficiently using a Probabilistic Turing Machine (PTM);
- Quantum Extended Church-Turing Thesis (QECTT): any realistic computing device can be simulated efficiently by a Fault-Tolerant Quantum Computer (FTQC).

CNOT gate

A CNOT (Controlled NOT) gate (aka CX gate) is a quantum gate[3] operating on two qubits, the target qubit and the control qubit. It inverts the state of the target qubit conditioned by the state of the control qubit. The CNOT quantum gate is considered the quantum computing equivalent of the classical computing XOR (eXclusive OR) gate as it flips the value of the target qubit if the quantum state of the control qubit is $|1\rangle$.

If the control qubit is in a superposition state (typically by applying an H gate), the target and control qubits become entangled.

combinatorial optimisation

Combinatorial optimisation consists of finding an optimal object from a finite set of objects, where the set of feasible solutions is discrete or can be reduced to a discrete set. Typical combinatorial optimisation problems are the Travelling Salesman Problem (TSP), the Minimum

[3] Formerly called Feynman gate (C).

Spanning Tree Problem (MSTP), and the knapsack problem. In many such problems, exhaustive search is not tractable, and so specialised algorithms that quickly rule out large parts of the search space or approximation algorithms must be resorted to instead.

complex number

A complex number is a number z that can be written in the form $z = a + bi$, where a (the real part) and b (the imaginary part) are real numbers and i is the imaginary unit defined by $i^2 = -1$. There are three ways to represent a complex number z:

1. Cartesian form: $z = (a, b)$ (a vector in a 2-dimensional plane);
2. polar form: $z = r\,(cos\theta + i\ sin\ \theta)$ where $r = |z|$ (the norm or modulus) and $\theta = arg(\theta)$ (the principal argument)[4];
3. exponential form: $z = r^{ei\theta}$.

The norm (or modulus) $|z|$ of a complex number $z = a + bi$ is the distance from the origin to the point (a, b) in a two-dimensional space. According to the Pythagorean theorem its value is:

$$\sqrt{a^2 + b^2}$$

Note that the square of the norm is always real number. For the complex numbers α and β that are the probability amplitudes corresponding with the quantum state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ of a qubit, the Born rule states that the sum of the squares of their norms, i.e. $|\alpha|^2 + |\beta|^2$ must be equal to 1.

computational basis

The computational basis refers to the basic states of a qubit or qubit register. For a single qubit (2^1 combinations), the computational bases are $|0\rangle$ and $|1\rangle$. For an n-qubit register (2^n combinations), the computational bases are $|00..0\rangle$ and $|11..1\rangle$.

computational complexity

The computational complexity of an *algorithm* is the amount of resources required to run it. Particular focus is given to time and memory requirements. The complexity of a *problem* is the complexity of the best algorithms that allow solving the problem.

[4] In quantum computing, θ is called the phase.

computational security

Computational security is based on the assumption that an adversary's computational resources (computing power and memory size) are insufficient to perform cryptanalysis or brute-force attacks.

Continuous Variable (CV)

A Continuous Variable (CV) is a variable whose value is obtained by measuring, i.e. one which can take on an uncountable set of values.

Controlled X (CX) gate

A Controlled X (CX) gate (aka CNOT gate) is a quantum gate operating on two qubits, the target qubit and the control qubit. It flips the value of the target qubit if the quantum state of the control qubit is |1⟩.

Cooper pair

A Cooper pair, aka Bardeen–Cooper–Schrieffer (BCS) pair, named after the American physicists John Bardeen, Leon N. Cooper and John Robert Schrieffer, is a pair of electrons bound together at very low temperatures. The electrons in a Cooper pair are not necessarily close together; because the interaction is long range, paired electrons may still be many hundreds of nanometres apart. This distance is usually greater than the average interelectron distance so that many Cooper pairs can occupy the same space. Therefore, unlike "common" electrons, multiple Cooper pairs are allowed to be in the same quantum state, which is responsible for the phenomenon of superconductivity.

crosstalk

Crosstalk is the effect where a "desired " operation on one or more qubits unintentionally affects one or more other qubits.

cryptanalysis

Cryptanalysis is used to break a cryptographic algorithm and obtain the cryptographic key that has been used, or gain access to the plaintext corresponding with encrypted data (ciphertext), even if the cryptographic key is not known.

In addition to mathematical attacks on cryptographic algorithms (aka algorithmic attacks), cryptanalysis includes the study of attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation and operation.

cryptographic hash function

A cryptographic hash function is a mathematical algorithm that maps data of an arbitrary size to a bitstring of a fixed size (the “hash” or "hash value"), by means of a one-way function. Ideally it should have the following properties:

- it is fast to compute the hash value for any given piece of data;
- the computed hash value is always the same for given piece of data, i.e. the hash function is deterministic;
- it is (practically) infeasible to generate a piece of data that yields a given hash value, i.e. it is impossible to reverse the process that generated the given hash value (pre-image resistance);
- for any given piece of data, it is (practically) infeasible to find another piece of data that has the same hash value (second pre-image resistance);
- it is (practically) infeasible to find (at least) two different pieces of data that have the same hash value (collision resistance);
- a small change to a piece of data should change its hash value so extensively that the new hash value appears uncorrelated with the old hash value (avalanche effect).

cryptographic security protocol

A cryptographic security protocol such as for example Transport Layer Security (TLS) describes how the encryption algorithms like AES and RSA should be used. A cryptographic security protocol specification includes details about data structures, representations and whether it can be used with interoperable versions.

Cryptographically Relevant Quantum Computer (CRQC)

The term Cryptographically Relevant Quantum Computer (CRQC) is used to specifically describe powerful future quantum computers that are capable of actually attacking real world cryptographic schemes that would be infeasible to attack with a classical computer.

declarative programming

Declarative programming is a programming paradigm that expresses the logic of a computation without describing its control flow. Many languages that apply this style attempt to minimise or eliminate side effects by describing what the program must accomplish in terms of the problem domain, rather than describing how to accomplish it as a sequence of the programming language primitives (the “how” being left up to the language's implementation).

Denial-of-Service (DoS)

A Denial-of-Service (DoS) attack is an attack which disrupts computing or networking services, so that these become temporarily or indefinitely unavailable to their intended users.

density matrix

A density matrix is a matrix that describes the quantum state of a quantum system. It allows for the calculation of the probabilities of the outcomes of any measurement performed upon this system.

A density matrix is a generalisation of the more usual quantum state vector or quantum wavefunction: while these can only describe a “pure” quantum state, a density matrix can also describe a “mixed” quantum state, when quantum subsystems are entangled or when the pure quantum state “decoheres” by interactions with the environment (this is for example the case with “noisy” qubits).

dequantization

Dequantization generally refers to the process of taking a proposed quantum algorithm and constructing a classical algorithm that typically has only a polynomial slowdown compared with the quantum algorithm. It is sometimes referred to as "quantum-inspired" algorithm.

device-independent quantum cryptography

Quantum cryptographic protocols are device-independent if their security does not rely on trusting that the quantum devices used to implement the protocol are truthful. The security analysis of these protocols includes scenarios of imperfect or even malicious devices.

Device-independent quantum cryptography is based on "self-testing" quantum devices, the internal operations of which can be uniquely determined by their input-output statistics. Bell inequality tests are typically used for checking the “honesty” of the quantum devices.

Several unconditionally secure device-independent quantum protocols have been proposed, even taking into account that the actual devices performing the Bell inequality tests may not be ideal (i.e. “noisy”).

differentiable programming

Differentiable programming is a programming paradigm in which a computer program can be differentiated throughout via automatic differentiation. This allows for gradient-based optimisation of parameters in the program, often via gradient descent, as well as other learning approaches that are based on higher-order derivative information.

Most differentiable programming frameworks, such as for example TensorFlow, work by constructing a graph containing the control flow and data structures in the program.

Diffie-Hellman (DH)

Diffie–Hellman (DH) was conceived by the American computer scientist and mathematician Ralph C. Merkle and named after the American cryptographers and mathematicians Bailey Whitfield Diffie and Martin Edward Hellman. It was the earliest practical example of public-key cryptography, followed shortly afterwards by the Rivest-Shamir-Adleman (RSA) proposal. The security of DH cryptography is based on the difficulty of solving the Discrete Logarithm Problem (DLP).

The DH key exchange algorithm allows two parties that have no prior knowledge of each other to jointly establish a shared secret symmetric encryption key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric encryption algorithm.

Although the DH key exchange protocol itself is non-authenticated, it provides the basis for a variety of authenticated key exchange protocols, and is used to provide forward secrecy in Transport Layer Security (TLS) ephemeral modes (referred to as Ephemeral Diffie-Hellman (EDH) or Diffie-Hellman Ephemeral (DHE).

Digital Annealer (DA)

A Digital Annealer (DA) is a dedicated digital computing chip that use a non-Von Neumann architecture to minimise data movement in solving combinatorial optimisation problems. Such a chip is composed of thousands of bit-updating blocks with on-chip memory that stores weights and biases, logic blocks to perform bit flips, and interfacing and control circuitry.

Rather than programming the DA, a problem is uploaded in the form of weight matrices and bias vectors so as to convert the problem into an “energy landscape”. Problem solving with a DA is very similar to problem solving with a Quantum Annealer (QA).

digital signature mechanism

A digital signature is the electronic analogue of a hand-written signature and must satisfy the following requirements:

- the receiver should be able to validate the sender’s signature;
- the signature must not be forgeable;
- the sender must not be able to successfully repudiate the signing of a message.

A major difference between digital (electronic) signatures and hand-written signatures is that a digital signature cannot be constant. Given its digital nature (a string of bits), a constant digital signature could easily be attached (copied) to any piece of data. A usable digital signature therefore needs to be a function of the entire piece of data (message, document, file, etc.) that is signed by it. Furthermore, digital signatures often include sequence numbers, timestamps etc., to ensure different digital signatures for otherwise equal pieces of data.

Most digital signatures are based on public-key cryptography schemes, many of which are based on specialised algorithms that are not suitable for encipherment purposes. It is usually not desirable to apply a digital signature directly to a possibly long piece of data, given the inefficiency of public-key encryption. Nonetheless, the entire piece of data should be protected by the signature. A way of satisfying both requirements is to use a cryptographic hash function as an intermediary. The hash function takes the entire piece of data and produces a fixed-length message digest (hash value), which is then digitally signed.

Discrete Logarithm Problem (DLP)

Discrete logarithms are defined with regard to multiplicative cyclic groups. If *G* is a multiplicative cyclic group and *g* is a generator of *G*, every element *h* in *G* can be written as g^x for some *x*. The discrete logarithm to the base *g* of *h* in the group *G* is defined to be *x*. The Discrete Logarithm Problem (DLP) is defined as: given a group *G*, a generator *g* and an element *h* of the group *G*, find the discrete logarithm to the base *g* of *h* in the group *G*.

Note

DLP is not always a hard problem: the hardness of finding discrete logarithms depends on the properties of the group.

Discrete Variable (DV)

A Discrete Variable (DV) over a particular range of real values is one for which, for any value in the range that the variable is permitted to take on, there is a positive minimum distance to the nearest other permissible value.

dispersion

In optical transmission, dispersion is the phenomenon in which the phase velocity of a wave depends on its frequency. An important consequence of dispersion is the change in the angle of refraction of different colours of light (the most familiar example of dispersion is a rainbow).

domain parameter

Domain parameters are parameters used with a cryptographic algorithm that are common to a domain of users of that algorithm.

Domain Specific Language (DSL)

A Domain Specific Language (DSL) is a language specialised to a particular application domain. This is in contrast to a general-purpose language, which is broadly applicable across application domains. DSLs can be further subdivided by the kind of language, and include domain-specific markup languages, domain-specific modelling languages (more generally, specification languages), and domain-specific programming languages.

Dominating Set Problem (DSP)

The Dominating Set Problem (DSP) concerns testing whether $\gamma(G) \leq K$ for a given graph G and input K; it is a classical NP-complete decision problem in computational complexity theory. Therefore it is believed that there may be no efficient algorithm that can compute $\gamma(G)$ for all graphs G.

Dynamical Decoupling (DD)

Dynamical Decoupling (DD) is an open-loop quantum control technique employed in quantum computing to suppress decoherence by taking advantage of rapid, time-dependent control modulation. In its simplest form, DD is implemented by periodic sequences of instantaneous control pulses, whose net effect is to approximately average the unwanted system-environment coupling to zero.

dynamic quantum circuit

Dynamic circuits allow for the interaction of real-time classical computation with the quantum computation by using intermediate (mid-circuit) measurements.

eigenstate and eigenvalue

The word "eigenstate" is derived from the German word "eigen", meaning "inherent" or “characteristic". An eigenstate is the measured state of some object possessing quantifiable characteristics such as position, momentum, etc. The state being measured and described must be observable (i.e. something such as position or momentum that can be experimentally measured either directly or indirectly), and must have a definite value, called an eigenvalue.

In the everyday world, it is natural and intuitive to think of every object being in its own eigenstate; this is just another way of saying that every object appears to have a definite position, a definite momentum, a definite measured value and a definite time of occurrence. However, in quantum mechanics, Heisenberg's uncertainty principle implies that it is impossible to measure the exact value for the momentum of a particle, given that its position has been determined at a given instant and likewise, it is impossible to determine the exact location of that particle once its momentum has been determined at a particular instant. Therefore, it becomes necessary to formulate clearly the difference between the state of something that is uncertain and the state of something having a definite value. When an object can definitely be "pinned down" in some respect, it is said to possess an eigenstate.

Einstein-Podolsky-Rosen (EPR) paradox

The Einstein-Podolsky-Rosen (EPR) paradox refers to a thought experiment that the Swiss-American theoretical physicist Albert Einstein, the Russian-American physicist Boris Yakovlevich Podolsky and the American-Israeli physicist Nathan Rosen formulated in 1935, in order to argue that quantum mechanics was an incomplete theory. In their view (which was shared by many other leading physicists at the time), quantum particles carry physical attributes not included in the quantum mechanics theory, and the uncertainties in quantum mechanics theory's predictions are due to ignorance of these attributes (which were later called 'local hidden-variables').

electromagnetic radiation

Electromagnetic radiation can be described in terms of a stream of mass-less particles, called photons, traveling in a wave-like pattern (at the speed of light in a vacuum). Electromagnetic radiation can be expressed in terms of energy, wavelength or frequency. The photons of the different types of radiation have different amounts of energy (measured in electron volts): radio waves have photons with low energies, microwave photons have a little more energy than radio waves, infrared light photons have still more, then comes visible light, ultraviolet light, X-rays and gamma-rays. The wavelength is measured in metres: 10 cm or more for radio waves, between 1 mm and 10 cm for microwaves, between 1 µm and 1 mm for infrared light, between 100 nm and 1 µm for visible light, between 10 nm and 100 nm for ultraviolet light, between 10^{-2} nm and 10 nm for X-rays, and 10^{-2} nm or smaller for gamma-rays. The frequency is the inverse of the wavelength and is measured in cycles per second (or Hertz).

electron

The electron is an elementary fermion subatomic particle with spin 1⁄2. The electron’s electric charge is negative one elementary charge (which is the electric charge carried by a single proton). Electrons play an essential role in numerous physical phenomena, such as electricity and magnetism.

elliptic curve

An elliptic curve that is used for cryptography purposes is the set of points that satisfy a mathematical equation with two variables, with degree two in one of the variables and degree three in the other (the so-called short Weierstrass form, named after the German mathematician Karl Theodor Wilhelm Weierstraß), for example: $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$ (this condition ensures that there are no singular points).

Elliptic curves have several interesting properties. One of them is that any non-vertical line will intersect the curve in at most three places. If one takes two points on the curve and draws a line through them, it will intersect the curve at exactly one more place. Put in other words: any two points on a curve can be “dotted” together to get a new point on the curve. One can also "dot" a point with itself multiple times. It turns out that if one takes an initial point "dotted" with itself n times to arrive at a final point, finding out the value of n when only the first and final point are known is a hard problem. This hard problem underlies Elliptic Curve Cryptography (ECC).

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-ECC cryptography to provide equivalent security. The security of ECC cryptography is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP).

Elliptic Curve Discrete Logarithm Problem (ECDLP)

The Elliptic Curve Discrete Logarithm Problem (ECDLP) is a special case of the Discrete Logarithm Problem (DLP) in which the cyclic group G is represented by the group P of points on an elliptic curve. Note that “elliptic curve discrete logarithm” is a misnomer because the discrete logarithm applies to multiplicative cyclic groups, while elliptic curve groups are additive cyclic groups. Nonetheless, almost everyone uses this wrong terminology.

elliptic curve isogeny

An elliptic curve isogeny is a non-constant function, defined on an elliptic curve, that takes values on another elliptic curve and preserves point addition. Elliptic curve endomorphisms (morphisms from a mathematical object to itself) are isogenies from an elliptic curve to itself. These isogenies are a source of exponentially-sized graphs, which connects nodes on a ring, with each node represents a particular endomorphism. These graphs are well connected so that any node in the graph can be reached in a few steps from (almost) any other node (this is called "rapid mixing"); these steps constitute a (short) path. There are no known efficient classical or quantum algorithms to recover such paths from endpoints; this is the hard problem on which isogeny-based cryptography relies.

entanglement distribution

Entanglement distribution refers to the distribution of entangled states across a quantum network.

entanglement purification

Entanglement purification is a mechanism recovering a nearly pure copy of an unknown pure quantum state using multiple noisy copies of that quantum state.

entanglement swapping

Entanglement swapping refers to the transfer of entanglement from a priori entangled systems to a priori non-entangled systems. It can also be used for the creation of multipartite entangled states from bipartite entanglement. Entanglement swapping is a very useful tool for entanglement purification and quantum teleportation, and as such plays an important role in quantum computing and quantum cryptography.

entanglement witness

An entanglement witness is an Hermitian operator which helps to decide whether a quantum state is entangled or not. The basic idea is that the expectation value of the witness will be different for separable and entangled quantum states.

entropy

Entropy is a scientific concept as well as a measurable physical property that is most commonly associated with a state of disorder, randomness or uncertainty.

Euler’s formula

A complex number z with radius 1 and angle θ (polar coordinates) can be expressed as

$z = e^{i\theta} = \cos(\theta) + i \sin(\theta)$.

It is named after the Swiss mathematician Leonhard Euler.

Euler’s number (*e*)

Euler’s number *e*, named after the Swiss mathematician Leonhard Euler, is a mathematical constant which is the base of natural logarithms. It is the limit of $(1 + 1/n)^n$ as n approaches infinity. Its value is 2.718281828459045…

Fault-Tolerant Quantum Computer (FTQC)

The quantum threshold theorem (aka quantum fault-tolerance theorem) states that a quantum computer with a physical error rate below a certain threshold can, through application of Quantum Error Correction (QEC) schemes, suppress the logical error rate to arbitrarily low levels. Such quantum computers are known as Fault-Tolerant Quantum Computers (FTQCs).

fermion

There are two fundamental classes of subatomic particles: fermions and bosons. A fermion is a subatomic particle whose spin quantum number is an odd half-integer value (1⁄2 , 3⁄2 , 5⁄2 , etc.). Some fermions (e.g. the electron and the quarks) are elementary subatomic particles (with spin 1⁄2), other fermions (e.g. the proton and the neutron) are composite subatomic particles made up of smaller constituents.

Elementary fermions are divided into two groups: those that must bind together (quarks) and those that can exist independently (leptons). According to the so-called Pauli exclusion principle (named after Wolfgang Pauli), fermions cannot occupy the same place at the same time; this leads to the common idea that "matter takes up space". The name fermion is in honour of Enrico Fermi, an Italian (later naturalised American) physicist who was the creator of the world's first nuclear reactor.

fermionic simulation

Simulating quantum physics with a device which itself is quantum mechanical, a notion originated by the American theoretical physicist Richard Feynman, would be an unparalleled computational resource. However, the universal quantum simulation of fermionic systems is daunting due to their particle statistics, and Feynman left as an open question whether it could be done, because of the need for physically implementing non-local control.

Quantum simulation of fermionic models is highly desirable, as classically computing the properties of interacting particles is classically intractable except for very small systems. The key to quantum simulation is mapping a model Hamiltonian onto a physical system. When the physical system natively mimics the model, the mapping can be direct and simulations can be performed using analogue techniques.

Fiat-Shamir (FS) heuristic

Most Zero-Knowledge Proof (ZKP) mechanisms are interactive, meaning that the provers require a response from the verifiers before they can complete their proof, which is not suitable for many applications. Fortunately, provers can avoid this by using the Fiat-Shamir heuristic (sometimes referred to as the Fiat-Shamir transformation). The idea behind the Fiat-Shamir heuristic is that instead of having the verifier send a random challenge value to the prover, the prover can compute this value itself by using a random function, such as a cryptographic hash function.

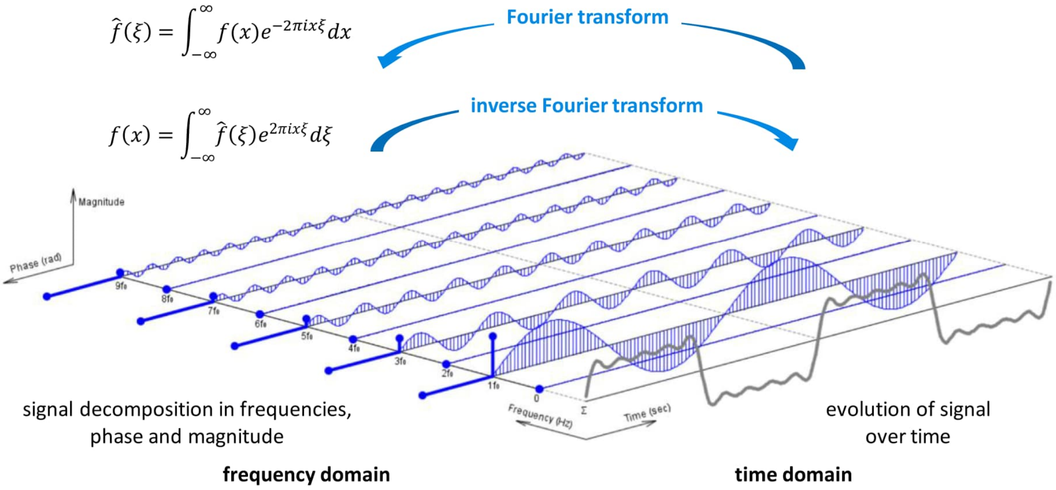
The Fiat-Shamir heuristic is named after the Israeli computer scientists Amos Fiat and Adi Shamir.

Fock space

The Fock space is the quantum state of boson many-body systems having the same quantum state. It is named after the Russian physicist Vladimir Fock.

Fourier transform

The Fourier transform is a mathematical decomposition of a time domain signal into elementary single frequency signals with their frequency, amplitude and phase. It is a complex value function of time with, for each frequency, a magnitude (real part) and a phase offset (complex part) of the sinusoid of this elementary frequency. The inverse Fourier transforms that frequency decomposition function back into its original compound signal. Fourier series were created by the French mathematician and physicist Jean-Baptiste Joseph Fourier, as part of his work in the book 'The Analytical Theory of Heat' published in 1822.



$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x)e^{-2\pi i x \xi}dx$$

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\xi)e^{2\pi i x \xi}d\xi$$

(source: Olivier Ezratty 2021)

full state tomography

For most quantum algorithms, a series of runs of the corresponding quantum circuit (including qubit measurement), followed by averaging the outputs of these runs, will output after roundup the found computational states of the qubit register. Otherwise, many runs are needed to reconstruct the qubit register amplitudes.

For a quantum algorithm with a reasonable small number of qubits and for characterising the quality of a small group of qubits, it may be useful to compute either a histogram of the whole computational state vector or a so-called quantum state tomography which will reconstitute the density matrix of the quantum register (providing the statistical distribution for each computational basis state). Doing so requires many runs and the number of runs grows exponentially with the number of qubits. Full state tomography is a tool used by quantum researchers and quantum hardware designers.

function

A function f defined by $y = f(x)$ maps every element x in a set A (the domain of the function f) to another element y (the image of x under the function f) in a set B (the co-domain of the function f):

$f : A \rightarrow B$

A function must obey the following rules:

1. Every member of the domain must be mapped.
2. Every member of the domain cannot be mapped to more than one element in the co-domain.

All the images x of the function f form a set called the range.

For an *injective function* (aka one-to-one function) each element in the range is the image of only one element in the domain (but not every element in the co-domain needs to be in the range).

For a *surjective function* (aka onto function) the range of the domain of the function is equal to its co-domain.

A *bijective function* is both injective and surjective. A function is inversible if it is bijective.

functional programming

Functional programming is a programming paradigm where a program is constructed by applying and composing functions without describing the program's control flow. Function definitions are trees of expressions that map values to other values, rather than a sequence of imperative statements which update the running state of the program.

Fusion-Based Quantum Computing (FBQC)

Fusion-Based Quantum Computing (FBQC) is a type of universal quantum computing that is built on two primitive operations: generation of small constant-sized entangled resource states and projective entangling measurements, which are referred to as fusions. The central principle of FBQC is to construct fusion networks from resource states and fusion measurements. A fusion network forms the fabric of the computation on which an algorithm can be implemented by modifying the basis of at least some of the fusion measurements. Appropriately combining fusion measurement outcomes gives the output of the computation.

gate-based quantum computer

A gate-based quantum computer is a device that takes input data and transforms this input data according to a quantum circuit specification.

Gaussian Boson Sampling (GBS)

Boson sampling is a restricted model of non-universal quantum computation that explores possible usage of boson scattering to evaluate expectation values of permanents of matrices. The model consists of sampling from the probability distribution of identical bosons scattered by a linear interferometer. Although the problem is well defined for any bosonic particle, its photonic version is currently considered as the most promising platform for a scalable implementation of a boson sampling device, which makes it a non-universal approach to linear optical quantum computing.

Gaussian Boson Samling (GBS) is a photonic implementation of boson sampling using Gaussian input states, i.e. states whose quasi-probability distribution function is a Gaussian one (named after the a German mathematician, astronomer and physicist Johann Carl Friedrich Gauß).

GitHub

GitHub (a subsidiary of Microsoft) provides internet hosting for source code version control using Git (open-source software for tracking changes in a set of files). GitHub offers features for source code development projects, e.g. collaboration among programmers, task management, bug tracking, continuous integration and wikis. It is the largest source code host for open-source projects.

Goppa code

A Goppa code, named after the Russian mathematician Valery Denisovich Goppa, is a type of error-correcting code and is based on modular arithmetic, which is when a series of numbers increases towards a certain number and upon reaching that number, starts back over at zero again.

Greenberger–Horne–Zeilinger (GHZ)

A Greenberger–Horne–Zeilinger (GHZ) state, named after the American physicists Daniel M. Greenberger and Michael Allan Horne, and the Austrian physicist Anton Zeilinger, is a certain type of entangled quantum state that involves at least three subsystems (particle states, qubits or qudits).

Grover's algorithm

Grover's algorithm (aka quantum search algorithm) is a quantum algorithm for unstructured search, conceived by the Indian-American computer scientist Lov Kumar Grover. It finds with high probability the unique input to a black box function that produces a particular output value, using just $O(\sqrt{N})$ evaluations of the function, where N is the size of the function's domain.

Grover's algorithm provides only a quadratic speedup compared to classical computation, which needs at least $O(N)$ evaluations on average. However, even quadratic speedup is considerable when N is large, and Grover's algorithm can be therefore be applied to speed up broad classes of algorithms, e.g. symmetric cryptographic algorithms, hash functions and Message Authentication Codes (MACs). As a result, it is sometimes suggested that symmetric cryptography key lengths, cryptographic hash value lengths and MAC tag sizes should be doubled to protect against future quantum computing attacks.

Hadamard (H) gate

The Hadamard (H) gate is a quantum gate that operates on a single qubit. It creates a superposed quantum state between $|0\rangle$ and $|1\rangle$ in the qubit when starting with $|0\rangle$ or $|1\rangle$ quantum states. It is named after the French mathematician Jacques Salomon Hadamard.

Hadamard transform

The Hadamard transform, named after the French mathematician Jacques Salomon Hadamard, is a square matrix operator with 2^n real values. It is a generalised Fourier transform that performs an orthogonal, symmetric, involutive, linear operation on 2^n real, complex or hypercomplex numbers.

Hamiltonian

The Hamiltonian of a quantum system is an operator corresponding to the total energy of that system, including both kinetic energy and potential energy. Its spectrum, the system's energy spectrum or its set of energy eigenvalues, is the set of possible outcomes obtainable from a measurement of the system's total energy.

The Hamiltonian is named after the Irish mathematician, astronomer and physicist William Rowan Hamilton, who developed a revolutionary reformulation of Newtonian mechanics, known as Hamiltonian mechanics, which was historically important to the development of quantum physics.

Hamiltonian simulation

Hamiltonian simulation aka quantum simulation implements the evolution of a quantum state efficiently. Hamiltonian simulation was proposed by the American theoretical physicist Richard Feynman in 1982, when he proposed a quantum computer as a possible solution since the simulation of general Hamiltonians seem to grow exponentially with respect to the quantum system size.

Hamming code

Hamming codes, named after the American mathematician Richard Wesley Hamming, are a family of linear error-correcting codes. Hamming codes can detect one-bit and two-bit errors, or correct one-bit errors without detection of uncorrected errors.

Hardware Security Module (HSM)

A Hardware Security Module (HSM) is a cryptographic module in the form of a USB-stick, a plug-in card or an external device attached directly to a computer or via a network connection. An HSM safeguards and manages cryptographic keys (including random key generation), performs encryption/decryption functions, performs cryptographic functions for generation/verification of digital signatures, strong authentication, etc.

Heisenberg uncertainty principle

Heisenberg's uncertainty principle, named after the German theoretical physicist Werner Karl Heisenberg, is asserting a fundamental limit to the accuracy with which the values for certain pairs of physical quantities of a particle, such as position and momentum, can be predicted from initial conditions.

It is usually defined as follows:

$\Delta x \ \Delta p \geq \hbar/2$

where Δx is the position, Δp is the momentum and $\hbar$ is the reduced Planck constant (aka Dirac constant).

Hermitian matrix

An Hermitian matrix, named after the French mathematician Charles Hermite, is a matrix with real numbers in the diagonal and which can have complex numbers in the rest. An Hermitian matrix is equal to its conjugate transpose (aka transjugate, Hermitian conjugate or adjoint matrix), which is obtained by changing the sign of the imaginary part of its complex numbers.

Hermitian operator

An Hermitian operator, named after the French mathematician Charles Hermite, is a linear operator (called a self-adjoint operator in mathematics) on a vector space V that is equipped with positive definite inner product, which is usually notated as a bra and ket (Dirac notation).

High-Performance Computing (HPC)

High-Performance Computing (HPC) is a type of classical computing that uses supercomputers and computer clusters to solve advanced computation problems.

Hilbert space

Hilbert spaces, named after the German mathematician David Hilbert, allow the methods of linear algebra and calculus to be generalised from finite-dimensional Euclidean vector spaces to spaces that may be infinite-dimensional. Formally, an Hilbert space is a vector space equipped with an inner product that induces a distance function for which the space is a complete metric space. A qubit state is a vector in a 2-dimensional Hilbert space.

Holevo theorem

The Holevo theorem, named after the Russian mathematician Alexander Semenovich Holevo, states that only n bits of useful information can be retrieved from a register of n qubits.

homodyne versus heterodyne detection

Homodyne detection is a method of extracting information encoded as modulation of the phase and/or frequency of an oscillating signal, by comparing that signal with a standard oscillation that would be identical to the signal if it carried null information. "Homodyne" relates to the use of a single frequency, in contrast to the dual frequencies employed in heterodyne detection.

Identity (I) gate

The Identity (I) gate is a single-qubit quantum gate that leaves the basis quantum states $|0\rangle$ and $|1\rangle$ of a qubit unchanged.

imperative programming

Imperative programming is a programming paradigm that specifies statements to change a program's state. In much the same way that the imperative mode in natural languages expresses commands, an imperative program consists of commands for the computer to perform. Imperative programming focuses on describing how a program operates step by step, rather than on high-level descriptions of its expected results.

Index-Calculate Method (ICM)

The Index-Calculate Method (ICM) is a probabilistic algorithm for solving the Discrete Logarithm Problem (DLP).

indistinguishability

Indistinguishability relates to boson quantum objects (e.g. photons) that have the same quantum state in a given location and are impossible to separate with any measurement tool.

information-theoretic security

Information-theoretic security comes from the laws of quantum mechanics, which bound the amount of information that can be extracted from a quantum system, irrespective of measurement or computational operations.

Integer Factorisation Problem (IFP)

Integer factorisation is the decomposition of a composite integer number into a product of smaller integers. When the numbers are sufficiently large, no efficient non-quantum integer factorisation algorithm is known. However, it has not been proven that an efficient non-quantum algorithm does not exist. The hardest numbers of a given length to factor are semiprimes (a semiprime is the product of two prime numbers). The widely used Rivest-Shamir-Adleman (RSA) public-key cryptography algorithm relies on the presumed difficulty (hardness) of semiprime factorisation.

interferometer

Interferometers work by merging two or more sources of light to create an interference pattern, which can be measured and analysed; hence “Interfere-o-meter”, or interferometer.

Internet of Things (IoT)

Internet of Things (IoT) relates to smart sensors and other smart devices (e.g. a smart toilet seat that measures heartbeat rate, blood pressure, body weight, etc.), which connect and exchange data with other devices and systems over computer networks (including the internet).

intractable problem

An intractable problem is a problem for which there is no known efficient algorithm, i.e. an algorithm with polynomial complexity, for solving it.

ion

An ion is an atom or molecule with either more or less electrons than protons, resulting in an overall negative or positive electric charge. An anion is a negatively charged ion (an atom or molecule with more electrons than protons); a cation is a positively charged ion (an atom or molecule with fewer electrons than protons).

ion trap

An ion trap is a combination of electric or magnetic fields used to capture ions (electrically charged atoms or molecules), often in a system isolated from the external environment. Ion traps have a number of scientific uses such as mass spectrometry, basic physics research and controlling quantum states.

Ising Chain (IC)

The one-dimensional Ising model is a chain of n spins, each spin interacting only with its two nearest neighbours and with an external magnetic field.

Ising model

The Ising model or Lenz–Ising model, named after the German physicists Ernst Ising and Wilhelm Lenz, is a mathematical model of ferromagnetism in statistical mechanics. The model consists of discrete variables that represent magnetic dipole moments of atomic spins that can be in one of two states (+1 or −1). The spins are arranged in a graph, usually a lattice (where the local structure repeats periodically in all directions), allowing each spin to interact with its neighbours. Neighbouring spins that agree have a lower energy than those that disagree. The system tends to the lowest energy but heat disturbs this tendency, thus creating the possibility of different structural phases. The model allows the identification of phase transitions as a simplified model of reality.

Josephson junction

The Josephson effect, named after the British theoretical physicist Brian David Josephson, is a phenomenon that occurs when two superconductors are placed in proximity, with some barrier or restriction between them. It is an example of a macroscopic quantum phenomenon, where the effects of quantum mechanics are observable at ordinary, rather than atomic, scale. The Josephson effect produces a current, known as a supercurrent, that flows continuously without any voltage applied, across a device known as a Josephson junction, which consists of two or more superconductors coupled by a weak link. The weak link can be a thin insulating barrier (known as a superconductor–insulator–superconductor junction), a short section of non-superconducting metal or a physical constriction that weakens the superconductivity at the point of contact.[5]

Jupyter notebook

Jupyter notebook can colloquially refer to two different concepts, either the user-facing application to edit code and text, or the underlying file format which is interoperable across many implementations:

1. A Jupyter notebook is a web-based interactive computational environment, built using several open-source libraries, for creating notebook documents.
2. A Jupyter notebook document is a JavaScript Object Notation (JSON file), usually ending with the ".ipynb" extension. Its main parts are: metadata, notebook format and list of cells. Metadata is a data dictionary of definitions to set up and display the notebook. Notebook

[5] The NIST standard for one volt is achieved by an array of 20,208 Josephson junctions in series.

format is a version number of the software. List of cells are different types of cells for markdown (display), code (to execute) and output of the code type cells.

Key Derivation Function (KDF)

A Key Derivation Function (KDF) is used in cryptography to derive multiple secrets (KDF outputs) from one or more other secrets (KDF inputs). A KDF is often used in security protocols that require participants to rederive the same key several times and is therefore expected to be deterministic. A KDF is usually not designed to produce a lot of derived secrets.

key exchange mechanism

A key exchange (aka key establishment) mechanism is a method by which symmetric cryptographic keys are exchanged between two or parties.

Key transport (aka key distribution) is the process whereby one entity generates a secret key and then transfers that secret key by secure means to the other entity. Key agreement is the process of establishing a shared secret key between two entities in such a way that neither of them can predetermine the value of the shared secret key. Key transport usually involves non-interactive techniques while key agreement usually involves interactive techniques. Key transport protocols and key agreement protocols can be based on either symmetric or asymmetric cryptographic techniques.

In many cases, the shared secret key that is established by a key transport or key agreement mechanism is not directly used, but is subject to further processing in order to derive the cryptographic key(s) that is (are) used for subsequent encryption and/or decryption.

laser

A laser emits light through a process of optical amplification based on the stimulated emission of electromagnetic radiation (hence the name). Stimulated emission is a quantum phenomenon where energy is extracted from a transition in an atom or molecule. Lasers emit highly coherent light beams (photons). Spatial (or transverse) coherence allows a laser to be focused to a very small spot and to stay narrow over great distances (collimation). Temporal (or longitudinal) coherence allows a laser to emit light with a very narrow frequency spectrum or to produce ultrashort pulses of light with a broad spectrum but with verry small durations (e.g. a femtosecond).

lattice

A lattice is a poset (a poset is a partially ordered set), in which every pair of elements has both a least upper bound and a greatest lower bound. In other words, it is a structure with two binary operations: join and meet.

Light-Emitting Diode (LED)

A Light-Emitting Diode (LED) is a semiconductor light source that emits light when an electrical current flows through it. This is caused by electrons in the semiconductor that recombine with electron holes, releasing energy in the form of photons. The colour of the light emitted by the LED (which corresponds to the energy of the photons) is determined by the energy required for electrons to cross the band gap of the semiconductor (i.e. the minimum energy required to excite an electron from its bound state into a free state, where it can participate in conduction). White light is obtained by using multiple semiconductors or by applying a layer of light-emitting phosphor on the semiconductor's surface.

Linear Optical Quantum Computing (LOQC)

Linear Optical Quantum Computing aka Linear Optics Quantum Computation (LOQC) is a paradigm of quantum computation, allowing universal quantum computation under certain conditions. LOQC uses photons as information carriers, mainly uses linear optical elements, or optical instruments (including reciprocal mirrors and waveplates) to process quantum information, and uses photon detectors and quantum memories to detect and store quantum information.

linear algebra

Linear algebra is the branch of mathematics which concerns the solutions and the structure of solutions for linear equations.

A system of m linear equations in n unknowns $x_1, x_2, \ldots , x_n$ is a collection of equations of the form

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1$$

$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2$$

$$\ldots$$

$$a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m$$

where a_{ij} are the coefficients (fixed real or complex numbers) and b_i are also fixed real or complex numbers. A solution is a set of numbers s_i , such that, substituting $x_i = s_i$ for the unknowns, all of the equations above hold.

In modern mathematics, the presentation through vector spaces instead of systems of linear equations is generally preferred since it is more synthetic, more general (not limited to the finite-dimensional case) and conceptually simpler, although more abstract.

logarithm

The logarithm is the inverse function to exponentiation: the logarithm of a given number x is the exponent y to which another (fixed) number, the base b, must be raised, to produce that number x $(x = b^y)$.

Low-Density Parity-Check (LDPC)

Low-Density Parity-Check (LDPC) codes (aka Gallager codes) are linear error correcting codes, invented by Robert G. Gallager in 1960 at MIT. LDPC codes require computationally expensive iterative decoding and therefore went unused for decades. In 1993, the newly invented turbo codes demonstrated that codes with iterative decoding could far outperform other codes in common use. However, turbo codes were patented; this provoked renewed interest in LDPC codes, which exhibit similar performance but are patent-free. Meanwhile, the patent for turbo codes has expired, but LDPC codes are still being used for various purposes (including QEC and QKD) because of their technical merits.

Low-Earth Orbit (LEO)

A Low-Earth Orbit (LEO) is an earth-centred orbit below an altitude of about one-third of earth's radius. Most of the artificial objects currently in outer space are in the LEO zone. Objects in orbits that pass through this zone, even if they have an apogee further out or are sub-orbital, are carefully tracked since they present a collision risk to the many LEO satellites. All crewed space stations launched to date have been within LEO. Since the end of the US Apollo program in 1972, no human spaceflights have been beyond LEO.

Majorana qubit

In 1937, the Italian physicist Ettore Majorana predicted the existence of a new class of particles, called Majorana fermions, that are its own anti-particles. A Majorana qubit is a “designed anyon”[6], in which bound states can appear at the interface between insulators and superconductors. These Majorana bound states can be used to create topological qubits used by topological quantum computing.

matrix

A matrix is a rectangular array or table of numbers, symbols or expressions, arranged in rows and columns. The size of a matrix is defined by the number of rows and columns it contains. There is no limit to the number of rows and columns a matrix can have as long as they are positive integers. A matrix with m rows and n columns is called an $m \times n$ matrix, while m and n are called its dimensions. It can be seen as a group of vectors that all have the same dimensions (number of columns).

Matrices are subject to standard mathematical operations such as addition and multiplication.

The *transpose* matrix $A^\dagger$ of a matrix A is derived by interchanging its rows into columns (or equivalently, interchanging its columns into rows). A matrix is *symmetric* if $A = A^\dagger$.

The *conjugate* matrix $\bar{A}$ of a matrix A is derived by conjugating each of its elements, i.e. $z = a + bi \rightarrow \overline{z} = a - bi$.

A *unitary matrix* is a complex square matrix whose columns (and rows) are orthonormal[7]. A unitary matrix has the remarkable property that its inverse is equal to its conjugate transpose[8]. When used as a unitary operator on a vector whose norm is 1, the result will be a vector whose norm is also 1.

Unitary matrices form a group, where:

1. The identity matrix I is unitary;

2. Given two unitary matrices U and V, the product UV is unitary;

[6] As opposed to anyons in the natural state of matter.

[7] A set of vectors S is orthonormal if every vector in S has magnitude 1 and the set of vectors are mutually orthogonal.

[8] A unitary matrix whose entries are all real numbers is said to be orthogonal.

3. Given a unitary matrix U, its inverse U^{-1} exists and is unitary.

The *trace* Tr(A) of a matrix A is the sum of all the elements of its main diagonal.

Maximal Independent Set (MIS)

An independent set of an undirected graph is a subset U of nodes such that no two nodes in U are adjacent. An independent set is maximal if no node can be added to U without violating the independency property. Such a set is called Maximal Independent Set (MIS).

Maximum Cut Problem (MCP)

For a given graph, the maximum cut (aka max-cut) is a cut whose size is at least the size of any other cut. That is, it is a partition of the graph's vertices into two complementary sets S and T, such that the number of edges between S and T is as large as possible. Finding such a cut is known as the Maximum Cut Problem aka MaxCut Problem (MCP).

Measurement Device-Independent QKD (MDI-QKD)

In Measurement Device-Independent QKD (MDI-QKD) technology, neither endpoint (sender or receiver) is configured as an optical receiver (as is done in conventional QKD technology), but rather both endpoints are configured as optical transmitters. The two optical transmitters send photons to an intermediate node, called mid-station, which couples and measures the photons (using Bell inequality testing to ensure that the behaviour of the mid-station complies with the laws of quantum mechanics). The endpoints can then distil a shared secret key from the two-photon interference measurement results disclosed by the mid-station.

Measurement-Based Quantum Computing (MBQC)

Measurement-Based Quantum Computing (MBQC) is a quantum computing method that uses a high number of groups of pre-entangled qubits, called cluster states, embedded in two-dimensional grids in which qubit state readouts modify the grid structure and help create quantum gates. The last measured qubit gives the result of the algorithm. This technique is particularly useful with flying qubits like photons because it can be implemented in a highly parallel way and support the limited depth of quantum circuits allowed by this technology.

Merkle tree

A Merkle tree (aka hash tree), named after the American computer scientist and mathematician Ralph C. Merkle, is a binary tree in which every leaf node is labelled with the cryptographic hash of a data block, and every node that is not a leaf node (called a branch node, inner node, or inode) is labelled with the cryptographic hash of the labels of its child nodes. A Merkle tree allows efficient and secure verification of the contents of a large data structure. Demonstrating that a leaf node is a part of a given hash tree only requires computing a number of hashes proportional to the logarithm of the number of leaf nodes in the tree.

Mermin inequality testing

Mermin inequality testing, named after the American physicist Nathaniel David Mermin, extends the entanglement of double quantum states used in Bell inequality testing into an entanglement of a higher number of quantum states.

Message Authentication Code (MAC)

A Message Authentication Code (MAC) is used to verify the authenticity (and at the same time, to protect the integrity) of a piece of data (a file, a document, a message, etc.). A MAC provides message authentication provided that there exists mutual trust, but will not resist repudiation (because the mutual trust relationship breaks with repudiation).

microwave cavity

A microwave cavity is a special type of resonator, consisting of a closed (or largely closed) metal structure that confines electromagnetic fields in the microwave region of the spectrum. The structure is either hollow or filled with dielectric material.

microwave waveguide

A microwave waveguide is a special form of transmission line, which consists of a hollow metal tube. Unlike a typical transmission line (such as a coax cable), a waveguide has no centre conductor.

mode of operation

A block cipher is a cryptographic algorithm that operates only on a fixed-length groups of bits, called a block. A block cipher mode of operation is a scheme that prescribes how to repeatedly apply a block cipher's single-block operation to enable encryption and decryption of data the size of which exceeds the block size. Block cipher modes of operation may require an Initialisation Vector (IV) to be encrypted/decrypted as the very first block of the sequence, preceding the encryption/decryption of the first block of the data itself. The IV ensures that distinct ciphertexts are produced even when the same plaintext is encrypted multiple times independently with the same key (the IV value must either be non-repeating or random, depending on the mode of operation). Also, most modes of operation require the last part of the data to be padded to the block size, if the size of the data to be encrypted is not a multiple of the block size.

modular arithmetic

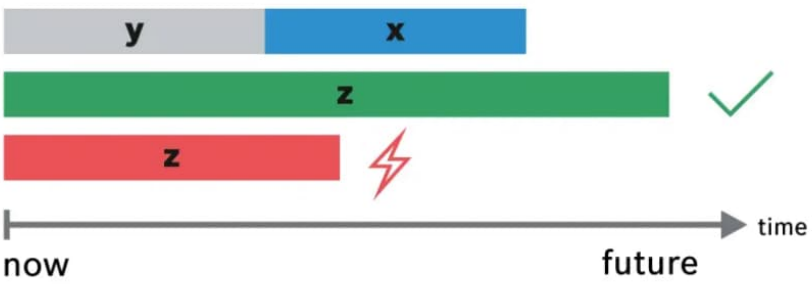
Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" when reaching a certain value, called the modulus. It was developed by the German mathematician, astronomer and physicist Carl Friedrich Gauß in 1801.

Monte Carlo sampling

Monte Carlo methods are a broad class of computational algorithms that rely on repeated random sampling to obtain numerical results. The underlying concept is to use randomness to solve problems that might be deterministic in principle. They are often used in physical and mathematical problems and are most useful when it is difficult or impossible to use other approaches. Monte Carlo methods are mainly used in three problem classes: optimisation, numerical integration and generating draws from a probability distribution.

Mosca theorem

The Mosca theorem (named after the Canadian mathematician and computer scientist Michele Mosca) helps to understand the timeline for post-quantum migration, i.e. updating systems and applications to quantum-secure cryptography.



If $x + y > z$ for a particular cryptographic scheme (i.e. a cryptographic algorithm using a set of particular parameters such as the key size), it will be vulnerable to attacks with a CRQC (Cryptographically Relevant Quantum Computer) at some point in the future.

x is the security shelf life; it refers to how long data encrypted with this particular cryptographic scheme must remain secure against quantum computing attacks after post-quantum migration has been completed;

y is the migration time; it refers to how much time will be needed to migrate from this particular cryptographic scheme to a quantum-secure cryptographic scheme;

z refers to the time when a quantum computer will be available that is capable of breaking this particular cryptographic scheme.

In other words: there is a problem if the time to migrate to a quantum-secure cryptographic scheme plus the security shelf life is beyond the time when a quantum computer will be capable of breaking the particular cryptographic scheme.

Multi-Party Computation (MPC)

Multi-Party Computation (MPC), also known as secure computation or privacy-preserving computation, relates to the use of cryptography for creating methods for parties to jointly compute a function over their inputs, while keeping those inputs private. Unlike most traditional usage of cryptography, where adversaries are outside the system of participants (such as an eavesdropper on the sender and receiver), MPC cryptography protects participants' privacy from each other.

multiplicative cyclic group

In modular arithmetic, the integers relatively prime to an integer n from the set $(0 , 1 , \ldots , n-1)$ of n non-negative integers form a group under multiplication modulo n, which is called the multiplicative cyclic group of integers modulo n.

multivariate equation

Multivariate equations are equations containing more than one variable. When faced with a multivariate equation, one may either wish to find a numeric value for each variable, or solve the equation for one variable in terms of the other variables.

native gate

A native gate is a quantum gate that is physically executed on quantum computer hardware.

neural network

A biological neural network is a network or circuit of neurons. An Artificial Neural Network (ANN) is composed of artificial neurons called nodes, for solving Artificial Intelligence (AI) problems. The connections of the biological neurons are modelled in ANNs as weights between nodes. A positive weight reflects an excitatory connection, while a negative weight reflects an inhibitory connection. All inputs to the ANN are modified by a weight and summed; this is referred to as a “linear combination”. An activation function controls the amplitude of the ANN's output.

neutral atom

Electrons and protons are electrically charged fermion subatomic particles. Electrons have negative electric charge, while protons have positive electric charge. A neutral atom is an atom where the charges of the electrons and the protons balance. The term “neutral atom” is commonly being used even though the word “neutral” is superfluous because an atom is neutral by definition (if it is not, it is called an ion).

neutral-atom qubit

In neutral-atom quantum computing, arrays of single neutral atoms are manipulated by light beams to encode and read out quantum states. In these types of quantum processors, a qubit is defined by one of two electronic states of an atom, and these single neutral atoms are arranged in configurable arrays.

neutron

The neutron is a fermion subatomic particle that has no electric charge and makes up the nucleus of an atom together with protons (except for hydrogen-1 which has no neutrons). A neutron is made of an up quark and two down quarks, held together by the strong force mediated by gluons.

Nitrogen-Vacancy centre (NV centre)

The Nitrogen-Vacancy centre (NV centre) is one of numerous point defects in diamond. Its most explored and useful property is its photoluminescence, which allows observers to read out its electron spin-state. The NV centre's electron spin can be manipulated at room temperature by magnetic fields, electric fields, microwave radiation or light, resulting in sharp resonances in the intensity of the photoluminescence.

NMR qubit

Nuclear Magnetic Resonance (NMR) qubits use the spin of atomic nuclei within large assemblies of molecules as their basis quantum states. Qubit readout is performed using nuclear magnetic resonance.

no-cloning theorem

The no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state. The no-cloning theorem has profound implications in the field of quantum computing and quantum communication.

Noisy Intermediate-Scale Quantum (NISQ)

Noisy Intermediate-Scale Quantum (NISQ) applies to current state-of-the-art quantum computers. The term 'noisy' refers to the fact that these quantum computers are very sensitive to the environment and may lose their quantum state due to quantum decoherence because they are not sophisticated enough to implement Quantum Error Correction (QEC). Quantum decoherence is the loss of quantum coherence and represents a challenge for the practical realisation of quantum computers, since such machines are expected to rely heavily on the undisturbed evolution of quantum coherences. The term 'intermediate-scale' refers to the not-so-large number of qubits.

The term NISQ was coined by the American theoretical physicist John Phillip Preskill in 2018.

norm of a complex number

The norm of a complex number $z = x + iy$, also called the modulus, is denoted $|z|$ and is defined as

$$|x + i\,y| \equiv \sqrt{x^2 + y^2}$$

.

Nuclear Magnetic Resonance (NMR)

Nuclear Magnetic Resonance (NMR) is a physical phenomenon in which nuclei in a strong constant magnetic field are perturbed by a weak oscillating magnetic field and respond by producing an electromagnetic signal with a frequency characteristic of the magnetic field at the nucleus. This process occurs near resonance, when the oscillation frequency matches the intrinsic frequency of the nuclei, which depends on the strength of the static magnetic field, the chemical environment, and the magnetic properties of the isotope involved.

nuclear spin

It is common practice to call the total angular momentum of the atom's nucleus "nuclear spin". For electrons in atoms a clear distinction is made between electron spin and electron orbital angular momentum, which is then combined to give the total angular momentum. But nuclei often act as if they are a single entity with intrinsic angular momentum. Associated with each nuclear spin is a nuclear magnetic moment which produces magnetic interactions with its environment.

Number Field Sieve (NFS)

The Number Field Sieve (NFS), aka General Number Field Sieve (GNFS), is the most efficient classical algorithm known for solving the integer factorisation problem for integers larger than 10^{100}. Until 2007, the gold-standard implementation was software developed and distributed by CWI in the Netherlands, which was available only under a relatively restrictive license. Jason Papadopoulos developed a faster public domain implementation in 2007. Both implementations feature the ability to be distributed among several nodes in a cluster with a sufficiently fast interconnect.

objective function

An objective function is either a cost function (aka loss function) or a profit function (aka reward function), which an optimisation problem seeks to minimise (cost function) or maximise (profit function).

One-Time Pad (OTP)

The One-Time Pad (OTP) cipher is a symmetric cryptography scheme that is based on the use of a single-use pre-shared secret key. A plaintext is paired with the secret key and each bit of the plaintext is encrypted by combining it with the corresponding bit from the secret key using modular addition (also known as XOR-ing). The resulting ciphertext will be impossible to decrypt without having knowledge of the secret key, provided that the following conditions apply:

- the pre-shared secret key must be at least as long as the plaintext;
- the pre-shared secret key must be perfectly random: the number of bits of entropy in the key must be at least equal to the number of bits in the plaintext (use of cryptographic hash functions or mathematical functions to generate secret keys with fewer bits of entropy would preclude perfect secrecy);
- the pre-shared secret key must never be reused in whole or in part;
- the pre-shared secret key must be kept completely private by the communicating parties.

OTP ciphers have been and are being used by nations for critical diplomatic and military communication, but the problems of secure secret key distribution and one-time key use render them impractical for most other use cases.

one-way function

A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input (where “easy" and "hard" relate to computational complexity). The existence of one-way functions is still being debated.

optical fibre

An optical fibre is a flexible, transparent fibre made by drawing glass (silica) or plastic to a diameter slightly thicker than that of a human hair. Optical fibres are commonly used as a means to transmit light (photons) between the two ends of the fibre and are used in fibre-optic communications, where they permit transmission over longer distances and at higher bandwidths than electrical cables, because signals travel along them with less loss and because they are immune to electromagnetic interference.

P versus NP problem

The P versus NP problem is considered by many to be the most important open problem in computer science. It asks whether every problem whose solution can be quickly verified can also be solved quickly. The informal term ‘quickly’ means the existence of an algorithm solving the task that runs in polynomial time (as opposed to, say, exponential time), such that the time to complete the task varies as a polynomial function on the size of the input to the algorithm which solves the problem instance. The class of questions for which some algorithm can provide an answer in polynomial time is P (Polynomial). For some questions, there is no known way to find an answer quickly, but if one is provided with information showing what the answer is, it is possible to verify the answer quickly. The class of questions for which an answer can be verified in polynomial time is NP (Nondeterministic-Polynomial).

parametron

A parametron is a logic circuit element invented by the Japanese computer scientist Eiichi Goto in 1954. The parametron is essentially a resonant circuit with a nonlinear reactive element which oscillates at half the driving frequency. The oscillation can be made to represent a binary digit by the choice between two stationary phases π radians (180 degrees) apart.

Parametrons were used in early Japanese computers due to being reliable and inexpensive but were ultimately surpassed by transistors due to differences in speed.

Pauli exclusion principle

The Pauli exclusion principle, named after the Austrian theoretical physicist Wolfgang Ernst Pauli, postulates that two fermion particles of the same kind cannot be in the same quantum state. For example, two electrons or two neutrons cannot be in the same place with the same energy level. If an external force such as gravitation forces them to be in the same place, they cannot have the same energy (i.e. the same speed). If a set of fermions has to be in the same place, they must have different energy levels.

Pauli gate

The Pauli X, Y and Z quantum gates operate on a single qubit. They perform a rotation, respectively, around the x, y and z axes of the Bloch sphere.

photon

The photon is an elementary subatomic particle. It is the quantum of the electromagnetic field, including electromagnetic radiation such as light and radio waves, and it is the force carrier for the electromagnetic force. Photons do not have electrical charge, they have zero mass and zero rest energy, and they only exist as moving particles. Photons move at 299,792,458 metres per second in a vacuum, the so-called “speed of light” denoted by *c* (from the Latin *celeritas*). The speed of photons in a medium depends upon the medium and is always slower than the speed in vacuum *c*.

photonic qubit

Photonic qubits use particles of light to carry and process information. Linear Optical Quantum Computing (LOQC) represents the common approach to quantum computing based on the use of photonic qubits.

physical and logical qubits

Several companies created actual qubits. These qubits are constructed from different materials and operate in controlled environments as there are a lot of factors that can influence the reliability of the state of a qubit like heat, magnetism, light, etc. Error correction is needed to increase the qubit reliability. One way of performing error correction is to deploy multiple imperfect physical qubits which jointly form the representation of a logical qubit (aka noiseless qubit or error-proof qubit).

Physically Unclonable Function (PUF)

A Physically Unclonable Function (PUF) is a physical entity that is embodied in a physical structure and is easy to evaluate but hard to predict. All PUFs are subject to environmental variations such as temperature, supply voltage and electromagnetic interference, which can affect their performance. Therefore, rather than just being random, the real power of a PUF is its ability to be different between devices, but simultaneously to be the same for a specific device under varying environmental conditions.

Planck constants and Planck units

Planck constant: $h = 6.626 \times 10^{-34}$ Js.

Reduced Planck constant (aka Dirac constant): $\hbar = h/2\pi$).

Planck time: $t_p = 10^{-44}$ s (shortest time measurement); below this value any observation is impossible.

Planck length (aka Planck distance): $l_p = 1.616255(18)\ 10^{-35}$ m (shortest distance measurement[9]); below this value any observation is impossible.

Planck mass: $m_p = 2.176343\ 10^{-41}$ kg (maximum mass of an elementary particle).

These constants and units are named after the German theoretical physicist Max Karl Ernst Ludwig Planck.

PLOB bound

The Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound, named after the Italian physicists Stefano Pirandola, Ricardo Laurenzo, Carlo Ottaviani and Leonardo Banchi, defines the maximum Quantum Key Distribution (QKD) rates that can be achieved with repeaterless quantum communication.

[9] The two digits enclosed by parentheses are the estimated standard error associated with the reported numerical value.

polarisation

Polarisation is a property of transverse waves which specifies the geometrical orientation of their oscillations. In a transverse wave, the direction of the oscillation is perpendicular to the direction of motion of the wave (in contrast, in longitudinal waves, the displacement of the particles in the oscillation is always in the direction of propagation, so these waves do not exhibit polarisation). Transverse waves that exhibit polarisation include electromagnetic waves such as light waves and radio waves. An electromagnetic wave consists of a coupled oscillating electric field and magnetic field which are always perpendicular to each other; by convention, the polarisation of electromagnetic waves refers to the direction of the electric field. In linear polarisation, the fields oscillate in a single direction. In circular or elliptical polarisation, the fields rotate at a constant rate in a plane as the wave travels. The rotation can have two possible directions; if the fields rotate in a right-hand sense with respect to the direction of wave travel, it is called right circular polarisation, while if the fields rotate in a left-hand sense, it is called left circular polarisation. The spin of the photon spin is the quantum-mechanical description of light polarisation, where spin +1 and spin −1 represent two opposite directions of circular polarisation. Light of a defined circular polarisation consists of photons with the same spin.

Pollard's Rho

The British mathematician John M. Pollard conceived different versions of the so-called Pollard's Rho algorithm: for solving the integer factorisation problem, for solving the Discrete Logarithm Problem (DLP) and for solving the Elliptic Curve Discrete Logarithm Problem (ECDLP).

polynomial

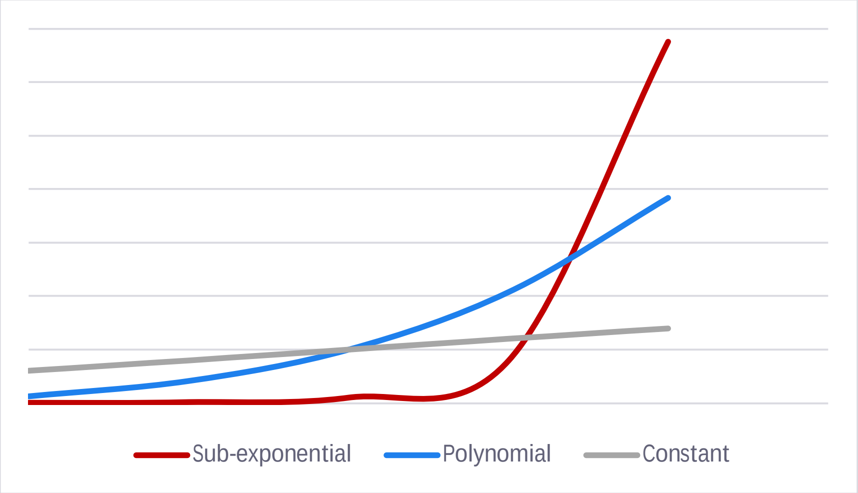
A polynomial is an expression consisting of variables and coefficients, which involves only the operations of addition, subtraction, multiplication and non-negative integer exponentiation of variables.

An example of a polynomial is $x^4 + 5xy^3 - 6yz + 3$.

polynomial time versus sub-exponential time

In computational complexity theory, polynomial time refers to the computation time of a problem where the run time, m(n), is no greater than a polynomial function of the problem size

n. Written mathematically using 'big O' notation, this states that $\mathbf{m(n)} = \mathbf{O(n^k)}$ where k is some constant that may depend on the problem.



For example, the classical 'quicksort' sorting algorithm on n integers performs at most $\mathbf{An^2}$ operations for some constant A. Thus it runs in $\mathbf{O(n^2)}$ time and is a polynomial time algorithm.

Sub-exponential time refers to the computation time of a problem where the run time is greater than a polynomial function but smaller than an exponential function of the problem size.

For example, the best-known classical algorithm for integer factorisation, the General Number Field Sieve (GNFS), runs in about $\mathbf{O(2^{\log n})^{\frac{1}{3}}}$ time for the factoring of an integer n.

Pre-Shared Key (PSK)

A Pre-Shared Key (PSK) is a secret key which was previously shared between two parties using a secure (typically out-of-band) communication channel, before it is put into use by some cryptographic mechanism.

projective measurement

Projective measurement is the most generic form of measurement used in quantum computing. The simplest case is a projection on the z-axis of the Bloch sphere, containing the |0⟩ and |1⟩ orthogonal vectors. Projective measurement on a qubit uses two orthogonal measurement operators in the form of a 2 x 2 Hermitian matrix[10].

[10] A Hermitian matrix (aka self-adjoint matrix) is a complex square matrix that is equal to its own conjugate transpose, i.e. the element in the i-th row and j-th column is equal to the complex conjugate of the element in the j-th row and i-th column.

Note that projective measurement operations are probabilistic and irreversible, in contrast to quantum gate operations, which are deterministic (giving the same results when executed several times[11]) and reversible.

proton

The proton is a fermion subatomic particle and makes up the nucleus of an atom together with neutrons. By definition, the proton's electric charge is positive one elementary charge. A proton is made of two up quarks and a down quark, held together by the strong force mediated by gluons.

Pseudo-Random Function (PRF)

A Pseudo-Random Function (PRF) is a family of efficiently-computable functions (e.g. polynomial-time computable functions) that emulate a random oracle in such a way that no efficient algorithm can distinguish between a function chosen randomly from the PRF family and a truly random oracle (a function whose outputs are fixed completely at random): if a function from the family is selected by choosing an input value uniformly at random, and one's knowledge of the selected function is limited to the output values corresponding to a feasible number of (adaptively) chosen input values, then the selected function is computationally indistinguishable from a function whose outputs were fixed uniformly at random.

A PRF family could be constructed from a Pseudo-Random Number Generator (PRNG) but PRFs should not be confused with PRNGs: the guarantee of a PRNG is that a single output appears random if the input was chosen at random, while the guarantee of a PRF is that all its outputs appear random regardless of how the corresponding inputs were chosen. In general, PRNGs do not constitute a PRF.

public-key cryptography

Public-key cryptography uses pairs of cryptographic keys. Each key pair consists of a public key (which may be known to others) and a private key (which must not be known by anyone except the owner). The generation of such key pairs depends on asymmetric cryptographic algorithms, which are based on hard mathematical problems (one-way functions).

[11] But of course modifying the qubit quantum state unless it was already a $|0\rangle$ or a $|1\rangle$.

Quadratic Unconstrained Binary Optimization (QUBO)

Quadratic Unconstrained Binary Optimization (QUBO) is a combinatorial optimisation problem with a wide range of applications from finance and economics to Machine Learning (ML). For many classical problems from theoretical computer science, embeddings into QUBO have been formulated. Embeddings for ML models include Support-Vector Machines (SVMs), clustering and probabilistic graphical models. Moreover, due to its close connection to the Ising model, QUBO constitutes a central problem class for Adiabatic Quantum Computing (AQC), where it is solved through an analogue process called quantum annealing.

quantum advantage

Quantum advantage is the goal of demonstrating that a quantum computer can solve a practical problem that no classical computer can solve in any feasible amount of time. Conceptually, quantum advantage involves both the engineering task of building a powerful quantum computer and the computational complexity-theoretic task of finding a problem that can be solved by that quantum computer and has a more than polynomial speedup over the best known or possible classical algorithm for that task.

quantum algorithm

A quantum algorithm is a step-by-step procedure, which is transformed into a quantum circuit that is executed by a quantum computer. Although classical algorithms can also be executed on a quantum computer, the term quantum algorithm usually designates algorithms that are inherently quantum (i.e. those that use some essential feature of quantum computation such as quantum superposition and quantum entanglement).

Quantum Amplitude Estimation (QAE)

Quantum Amplitude Estimation (QAE) is a quantum algorithm that retrieves information stored in the amplitude of a quantum state. It is argued to have a quadratic speedup over simple repeated sampling of the quantum state.

quantum annealing

Quantum annealing is a metaheuristic for finding the global minimum of a given objective function over a given set of candidate solutions, by a process using quantum fluctuations. A quantum fluctuation is the temporary random change in the amount of energy in a point in space as prescribed by Heisenberg's uncertainty principle. Quantum fluctuations are minute random fluctuations in the values of the fields which represent elementary particles, such as electric and magnetic fields. Although the particles are not directly detectable, the cumulative effects of these particles are measurable.

Quantum Approximate Optimization Algorithm (QAOA)

Mostly, an optimisation problem is formulated as a minimisation problem, where one tries to minimise an error which depends on the solution: the optimal solution has the minimal error. Different optimisation techniques are applied in various fields such as mechanics, economics and engineering, and as the complexity and amount of data involved rise, more efficient ways of solving optimisation problems are needed. Approximate optimisation is a way of finding an approximate solution to an optimisation problem. The power of quantum computing may allow optimisation problems which are not practically feasible on classical computers to be solved by means of Quantum Approximate Optimization Algorithms (QAOAs) or suggest a considerable speed up with respect to the best-known classical optimisation algorithm.

Quantum Bit Error Rate (QBER)

The Quantum Bit Error Rate (QBER) is the ratio of an error rate to the Quantum Key Distribution (QKD) key rate and contains information on the existence of an eavesdropper and how much he knows.

Quantum Characterization, Verification, and Validation (QCVV)

Quantum Characterization, Verification, and Validation (QCVV) refers to developing methodologies, tools and techniques to verify the behaviour of quantum processors, validate their results and assess their performance against theoretical expectations.

quantum circuit

A quantum circuit specifies a set of qubits and the sequence of operations to be performed on these qubits, i.e. preparation of qubits, quantum gate operations on the qubits and qubit measurements.

Quantum Computing-as-a-Service (QCaaS)

Quantum Computing-as-a-Service (QCaaS) is a cloud service that provides customers access to quantum computing platforms through the internet.

quantum dot

Quantum dots are semiconductor particles a few nanometres in size, having optical and electronic properties that differ from larger particles due to the laws of quantum mechanics.

quantum emulator

A quantum emulator is a software and/or hardware system using a conventional computer to run and test some software programmed for a quantum computer. This makes it possible to test quantum programs without a quantum computer. The execution speed is far less than on a quantum computer as soon as a few tens of qubits are exceeded. Beyond about fifty qubits, the capacity of classical computers is insufficient to perform quantum emulation properly.

Quantum emulation should not be confused with quantum simulation, which simulates quantum physics phenomena with an analogue quantum processor.

quantum entanglement

Quantum entanglement[12] is a physical phenomenon that occurs when a group of particles are generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the group cannot be described independently of the quantum state of the others, including when the particles are separated by a large distance. The topic of quantum entanglement is at the heart of the disparity between classical physics and quantum mechanics.

[12] The term “quantum entanglement” was introduced by the Austrian (later naturalised Irish) physicist Erwin Rudolf Josef Alexander Schrödinger, but “quantum correlation” would have been a better choice to describe this phenomenon.

Quantum Error Correction (QEC)

Quantum Error Correction (QEC) is used in quantum computing to protect quantum information in Fault-Tolerant Quantum Computers (FTQCs) from errors due to decoherence and other quantum noise.

Quantum Error Mitigation (QEM)

Quantum Error Mitigation (QEM) is a technique that reduces quantum computing errors by combining classical post-processing with quantum circuit modifications, running the quantum algorithm several times and averaging the single-run results. QEM is an intermediate solution for NISQ that aims at increasing the computational power of quantum computers while Fault-Tolerant Quantum Computers (FTQCs) are not yet available.

Quantum Fast Fourier Transform (QFFT)

Quantum Fast Fourier Transform (QFFT), aka Quantum Fourier Transform (QFT), is a linear transformation on qubits. It is the quantum analogue of the classical Fourier transform algorithm. QFFT is part of many quantum algorithms, in particular Shor's algorithm for solving the Discrete Logarithm Problem (DLP).

Quantum Flux Parametron (QFP)

A Quantum Flux Parametron (QFP) is a digital logic implementation technology based on superconducting Josephson junctions. QFP's were invented by the Japanese computer scientist Eiichi Goto as an improvement over his earlier parametron based digital logic technology, which did not use superconductivity effects or Josephson junctions. The Josephson junctions on QFP integrated circuits to improve speed and energy efficiency enormously over the parametrons.

A related technology is the Rapid Single Flux Quantum (RSFQ) digital logic.

quantum gate

A quantum gate applies a unitary matrix (aka unitary operator) to the quantum state vector of one or more qubits.

Single-qubit gates apply a 2x2 unitary matrix of complex numbers to the qubit state vector containing 2 entries (the α and β complex amplitudes). These quantum gates always generate some rotation of the qubit state vector in the Bloch sphere while he norm of the vector remains stable at 1, at least before any decoherence happens.

Two-qubit gates apply a 4x4 unitary matrix to the two-qubit state vector containing 4 entries.

Three-qubit gates apply an 8x8 matrix to the three-qubit state vector containing 8 entries.

More generally, n-qubit gates apply a 2^nx2^n unitary matrix to the n-qubit state vector containing 2^n entries.

It should be noted that quantum gates are reversible operations that modify the qubit(s) quantum information without measuring it.

quantum gate teleportation

Quantum gate teleportation is a quantum circuit construction where a gate is applied to target qubits by first applying the gate to an entangled state and then teleporting the target qubits through that entangled state.

quantum indeterminacy (Heisenberg principle)

Quantum indeterminacy (Heisenberg principle, named after the German theoretical physicist Werner Karl Heisenberg) is a fundamental principle of quantum mechanics which postulates that there is a lower limit to the precision with which one can measure two independent parameters relating to the same quantum object such as its speed and position or the energy emitted and the duration of emission.

quantum information

Quantum information is concerned with studying the way in which the laws of quantum mechanics can be used to store and process information and to perform computations. In particular, the possibility of creating quantum superpositions of classical states, and to create correlations without a classical correspondence, such as entanglement, give rise to a wide range of new phenomena in data processing and computation.

Quantum Intermediate Representation (QIR)

Quantum Intermediate Representation (QIR) is an intermediate representation for quantum programs developed by Microsoft. QIR is intended to serve as a common interface between quantum computing languages and quantum computer platforms.

Quantum Linear System Problem (QLSP)

The Quantum Linear System Problem (QLSP) refers to solving large systems of linear equations by encoding the solution in a quantum state.

Quantum Machine Learning (QML)

Quantum Machine Learning (QML) refers to quantum algorithms that solve tasks in Machine Learning (ML), thereby improving and often expediting classical ML techniques. Such algorithms typically require one to encode the given classical data set into a quantum computer to make it accessible for quantum information processing. Subsequently, quantum information processing routines are applied and the result of the quantum computation is read out by measuring the quantum system.

quantum measurement

A quantum measurement is the testing or manipulation of a quantum system to yield a numerical result. The predictions that quantum mechanics makes about these measurements are in general probabilistic and depends on state of the quantum system that is being measured. The main objective of quantum computing is to execute a quantum circuit to set up the system's quantum state in such a way that (the) desired measurement outcome(s) have a high probability of occurring.

quantum memory

Quantum memory is the quantum-mechanical version of classical computer memory. Whereas classical computer memory stores information as binary states, quantum memory stores quantum states for later retrieval. Unlike the classical computer memory states, the states stored in quantum memory can be in a quantum superposition.

Quantum Monte Carlo (QMC)

Quantum Monte Carlo (QMC) encompasses a large family of computational methods whose common aim is the study of complex quantum systems. One of the major goals of these approaches is to provide a reliable solution (or an accurate approximation) of the quantum many-body problem. The diverse flavours of QMC approaches all share the common use of the Monte Carlo method to handle the multi-dimensional integrals that arise in the different formulations of the many-body problem.

Quantum Non-Demolition (QND) measurement

Quantum Non-Demolition (QND) measurement is type of measurement in which the uncertainty of the measured observable does not increase from its measured value during the subsequent normal evolution of the system. QND measurements are the least disturbing type of measurement in quantum mechanics. For a qubit, it means that after a |0⟩ or |1⟩ is measured, subsequent measurements will always yield the same |0⟩ or |1⟩ that was obtained in the first place.

Quantum Phase Estimation (QPE)

The Quantum Phase Estimation (QPE) algorithm is used to estimate the phase corresponding to an eigenvalue of a given unitary operator. Because the eigenvalues of a unitary operator always have unit modulus, they are characterised by their phase, and therefore the algorithm can be equivalently described as retrieving either the phase or the eigenvalue itself. QPE is based on the Quantum Fourier transform (QFT) algorithm and is used as a subroutine in other quantum algorithms, such as Shor's algorithm and algorithms for solving the Quantum Linear Systems Problem (QLSP).

quantum Principal Component Analysis (qPCA)

quantum Principal Component Analysis (qPCA) is be used to analyse an unknown low-rank density matrix by rapidly revealing the principal components of it, i.e. the eigenvectors of the density matrix with the largest eigenvalues.

Quantum Processor Unit (QPU)

A Quantum Processor Unit (QPU) is the basic building block of a quantum computer. The QPU consists of a set of (partially) interconnected qubits and the interfaces that are needed for qubit initialisation, reset and readout, and for executing quantum gate operations.

quantum Random-Access Memory (qRAM)

A Random-Access Memory (RAM) uses n bits to randomly address $N = 2^n$ distinct memory cells. A quantum Random-Access Memory (qRAM) uses n qubits to address any quantum superposition of N memory cells. The memory array can be either quantum or classical, depending on the qRAM's usage.

Quantum Random Oracle Model (QROM)

Security proofs for digital signature schemes are typically presented in the Random Oracle Model (ROM). The ROM postulates a truly random function that is accessible to attackers only through "black box" queries to a suitable random oracle. A security proof for a digital signature scheme must substitute a specific choice of hash function for the random oracle. An attacker armed with a quantum computer can be expected to evaluate that hash function in quantum superposition. Arguments that establish security even against such quantum-enabled attackers are said to hold in the Quantum Random Oracle Model (QROM). It is conceivable that a signature scheme shown to be secure in the ROM may not be secure in the QROM. Thus, it is important that security arguments for quantum-resistant digital signature schemes hold not merely in the ROM, but also in the QROM.

quantum simulator

A quantum simulator is an analogue quantum computer that is capable of simulating quantum objects and solving related problems, particularly in materials physics.

Quantum simulation should not be confused with quantum emulation: quantum emulators are classical computer systems capable of executing quantum algorithms by performing numerical computations.

Quantum Singular Value Transformation (QSVT)

Quantum Singular Value Transformation (QSVT) uses a linear algebra technique known as block encoding and a generalisation of Quantum Signal Processing (QSP)[13] to transform matrices that are inside larger unitary matrices.

quantum state

A quantum state is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a quantum system. Knowledge of the quantum state together with the rules for the quantum system's evolution in time exhausts all that can be predicted about the quantum system's behaviour.

A distinction can be made between pure and mixed states of physical systems that we observe. Both pure states and mixed states describe the information we can extract from the system after performing repeated measurements on the system. The difference between pure and mixed states is related to the origin of the measurement randomness: it is entirely of a quantum nature for pure states[14] and of both a quantum and classical nature for mixed states.

A *pure state* is a state of an isolated physical system, which can be described by a single quantum state vector as a linear superposition of its computational basis states. Example: the pure state for a single-qubit quantum system is described as:

$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

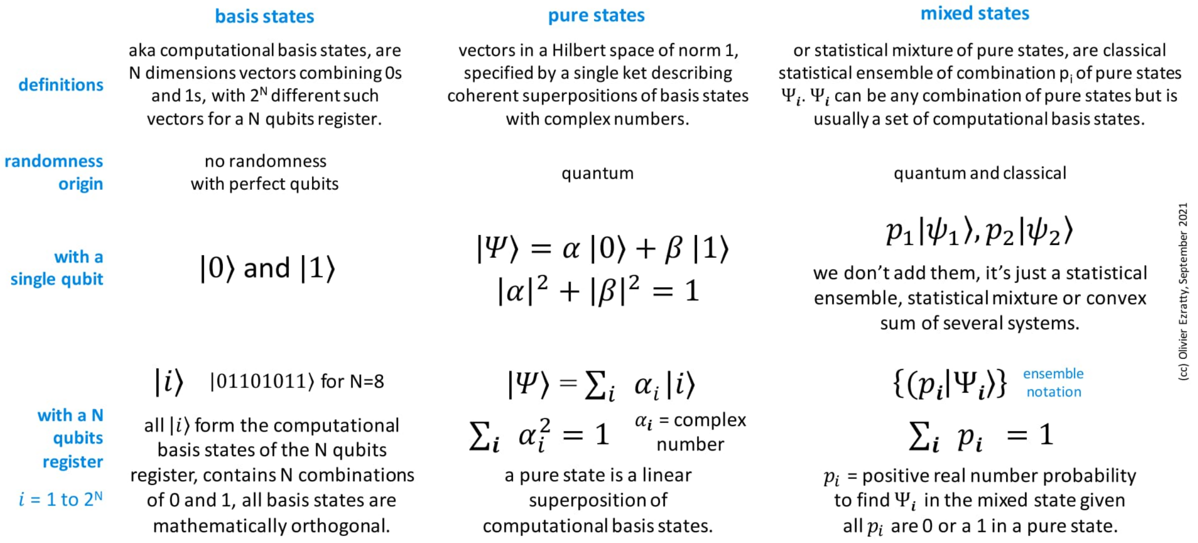
A unitary matrix (or operation) *U* acts on an arbitrary pure quantum state by conjugation[15]:

$|\Psi\rangle\langle\Psi| \longmapsto U|\Psi\rangle\langle\Psi|U^*$

[13] Quantum Signal Processing (QSP) is a Hamiltonian simulation algorithm with optimal lower bounds in query complexity. It linearises the operator of a quantum walk using eigenvalue transformation.

[14] A measurement performed on a physical system that is in a pure state generates random results most of the time; we have to prepare and measure it on a repeated basis to obtain its state probability distribution.

[15] Complex conjugation (aka conjugation) is an nonlinear operation that is performed on complex numbers. For a complex number z = a + bi , the conjugate is z* = a - bi .



	basis states	pure states	mixed states
definitions	aka computational basis states, are N dimensions vectors combining 0s and 1s, with 2^N different such vectors for a N qubits register.	vectors in a Hilbert space of norm 1, specified by a single ket describing coherent superpositions of basis states with complex numbers.	or statistical mixture of pure states, are classical statistical ensemble of combination p_i of pure states Ψ_i. Ψ_i can be any combination of pure states but is usually a set of computational basis states.
randomness origin	no randomness with perfect qubits	quantum	quantum and classical
with a single qubit	$\lvert 0\rangle$ and $\lvert 1\rangle$	$\lvert\Psi\rangle = \alpha\,\lvert 0\rangle + \beta\,\lvert 1\rangle$ $\lvert\alpha\rvert^2 + \lvert\beta\rvert^2 = 1$	$p_1\lvert\psi_1\rangle, p_2\lvert\psi_2\rangle$ we don't add them, it's just a statistical ensemble, statistical mixture or convex sum of several systems.
with a N qubits register i = 1 to 2^N	$\lvert i\rangle$ $\lvert 01101011\rangle$ for N=8 all $\lvert i\rangle$ form the computational basis states of the N qubits register, contains N combinations of 0 and 1, all basis states are mathematically orthogonal.	$\lvert\Psi\rangle = \sum_i \alpha_i \lvert i\rangle$ $\sum_i \alpha_i^2 = 1$ α_i = complex number a pure state is a linear superposition of computational basis states.	$\{(p_i\lvert\Psi_i\rangle\}$ ensemble notation $\sum_i p_i = 1$ p_i = positive real number probability to find Ψ_i in the mixed state given all p_i are 0 or a 1 in a pure state.

(cc) Olivier Ezratty, September 2021

A *mixed state* is a statistical ensemble of pure states. Mixed states arise in two different situations:

1. When one wants to describe a physical subsystem which is entangled with another subsystem[16].

2. When the preparation of a physical system is not fully known, and thus one must deal with a statistical ensemble of possible preparations[17].

A mixed state cannot be described with a single quantum state vector. Instead, it is described by its associated density matrix (aka density operator) ρ:

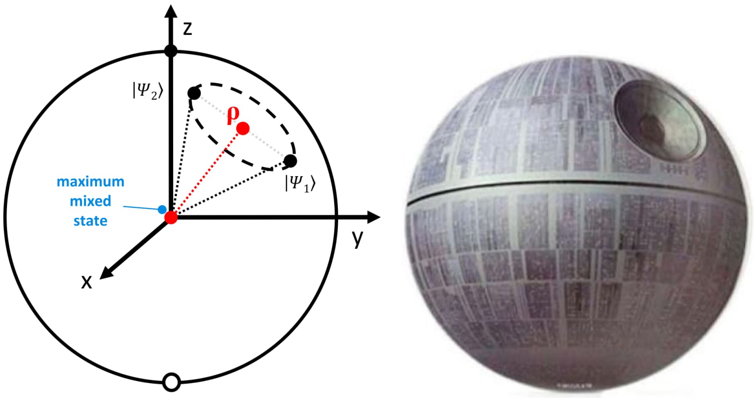
$\rho = p_1\lvert\Psi_1\rangle\langle\Psi_1\rvert + p_2\lvert\Psi_2\rangle\langle\Psi_2\rvert + \ldots$

where p_i is the probability associated with the pure state $\lvert\Psi_i\rangle$.

A unitary matrix (or operation) *U* acts on an arbitrary mixed state by conjugation: $\rho \mapsto U\rho U^*$

[16] Quantum entanglement prevents the existence of complete knowledge about the observed subsystem because it is not an isolated one: it is a subsystem of a larger entangled system. It is therefore not possible for an observer to describe the subsystem as a pure state. This is for example the case for qubits that are affected by decoherence caused by interactions with the environment, resulting in entanglement between the observed system and its environment.

[17] In this case, there could theoretically be another observer who could describe the same system as a pure state.



(source: Olivier Ezratty 2021)

Single-qubit mixed state can be represented by points inside the Bloch sphere with three degrees of freedom: its two angles ϕ and θ, and the vector length. A mixed state can result from an infinite number of combinations of various pure states as shown in the sphere. The state purity is measured by its proximity to the Bloch sphere surface. A maximum mixed state is at the centre of the Bloch sphere with equiprobability of |0⟩ and |1⟩.

Note

Density matrices can describe both mixed and pure states. A mixed state density matrix consolidates both quantum uncertainties and classical uncertainties, while a pure state density matrix contains only information pertaining to quantum uncertainties. For example, the density matrix of a quantum register that is in a pure state is the outer product of its computational basis state vector: $\rho = |\Psi\rangle\langle\Psi|$.

quantum state collapse

Quantum state collapse is one of two processes by which quantum systems evolve in time; the other is the continuous evolution via the Schrödinger equation. Quantum state collapse occurs when a wave function, which is initially in a superposition of several eigenstates, reduces to a single eigenstate due to interaction with the external world. This interaction is sometimes called an ‘observation’. It is the essence of a measurement in quantum mechanics, which connects the wave function with classical observables like position and momentum.

quantum state tomography

Quantum state tomography is a technique used to characterise the quality of qubits and quantum gates or any quantum channel. It is used to experimentally reconstruct a density matrix of a set of qubits. It also requires a lot of classical computing to process the experimental data obtained with repeated state preparation and measurements.

quantum state vector

A quantum state vector is a vector in an Hilbert space which represents the pure state of a quantum object.

quantum superposition

Quantum superposition[18] is a fundamental principle of quantum mechanics. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct quantum states. The principle of quantum superposition states that if a physical system may be in one of many configurations (arrangements of particles or fields) then the most general state is a combination of all of these possibilities[19]. The principle applies to the states that are theoretically possible without mutual interference or contradiction. It requires us to assume that between these states there exist peculiar relationships such that whenever the system is definitely in one state, we can consider it as being partly in each of two or more other states. The original state must be regarded as the result of a kind of superposition of the two or more new states, in a way that cannot be conceived on classical ideas. Any state may be considered as the result of a superposition of two or more other states, and indeed in an infinite number of ways.

quantum teleportation

Quantum (state) teleportation is a communication method that involves transmitting quantum information by exploiting the properties of quantum entanglement. It works by first creating pairs of entangled photons and then sending one photon of each pair to the sender and the other one to the receiver. The sender measures the quantum state of the photons that hold the quantum information and the state of the entangled photons at the same time. These interactions change the state of its photons, and because they are entangled with the receiver's photons, the interactions instantaneously change the state of the receiver's photons too. In effect, this "teleports" the quantum state in the sender's photons to the receiver's photons. However, the

[18] The term "superposition" was introduced by the British mathematician and theoretical physicist Paul Adrien Maurice Dirac, but "superimposition" would have been a better choice.

[19] Superposition is a consequence of wave-particle duality: waves can add with each other, but quantum objects are not "here" and "there" simultaneously as is often mistakenly assumed.

receiver cannot reconstruct the quantum information until the sender sends the result of its measurements in the form of classical bits (via optical fibre cables or other means).

quantum tunnelling

Quantum tunnelling is a quantum mechanical phenomenon in which a particle passes through a potential energy barrier that, according to classical mechanics, the particle does not have sufficient energy to enter or surmount[20]. Quantum tunnelling is a consequence of the wave nature of matter, where wave equations such as the Schrödinger equation describe the behaviour of a particle. The probability of transmission of a particle wave packet through a barrier decreases exponentially with the barrier height, the barrier width and the particle's mass, so tunnelling is seen most prominently in low-mass particles such as electrons or protons tunnelling through microscopically narrow barriers.

Quantum Turing Machine (QTM)

A Quantum Turing Machine (QTM) is an abstract machine used to model the effects of a quantum computer. It provides a simple model that captures all of the power of quantum computation, i.e. any quantum algorithm can be expressed formally as a particular QTM. Turing machine is named after the British mathematician, computer scientist, logician, cryptanalyst and philosopher Alan Mathison Turing.

quantum walk

In mathematics, a random walk (aka drunkard's walk) is a random process that describes a path that consists of a succession of random steps in some mathematical space. An example is a random walk on a regular lattice, where at each step the location jumps to another site according to some probability distribution. In a simple random walk, the location can only jump to neighbouring sites of the lattice, forming a lattice path. In a simple symmetric random walk on a

[20] The quantum tunnelling effect is not exploited in transistors as is often claimed. The widely used Metal-Oxide-Semiconductor Field-Effect Transistor (MOSFET) transistors (invented by Bell Labs in 1959) make use of the field effect (discovered by the Austrian-Hungarian-American physicist and electrical engineer Julius Edgar Lilienfeld in 1923).

locally finite lattice, the probabilities of the location jumping to each one of its immediate neighbours are the same.

Quantum walks are quantum analogues of classical random walks. In contrast to the classical random walk, where the walker occupies definite states and the randomness arises due to stochastic transitions between states, in quantum walks randomness arises through either:

- quantum superposition of states;
- non-random, reversible unitary evolution;
- collapse of the wave function due to state measurements.

quantum-dot qubit

Spin qubits in semiconductor quantum dots are formed when electrons or holes are confined in a static potential well in a semiconductor, giving them a quantised energy spectrum. The simplest spin qubit is a single electron spin located in a quantum dot, which is called quantum-dot qubit.

Quantum-Inspired Algorithm (QIA)

Quantum-Inspired Algorithms (QIAs) use classical computers to simulate some quantum phenomena in order to perform simulated quantum computations.

Quasi-Cyclic Moderate Density Parity-Check (QC-MDPC) code

Quasi-Cyclic Moderate Density Parity-Check (QC-MDPC) codes are variants of Moderate Density Parity-Check (MDPC) codes. MDPC allows for fast encoding and decoding while also being able to correct a lot of errors. The name originates from the appearance of the parity-check matrix. MDPC codes have parity-check matrices which contain a lot of zeroes and very few ones. The density of these parity-check matrices equal the percentage of ones in the entire matrix. MDPC codes have densities in the order of approximately 0.5% or more.

qubit (quantum bit)

A qubit (quantum bit) is a basic unit of quantum information. It is the quantum version of the classic bit (binary bit) physically realised with a two-state quantum device. In classical computing the information is encoded in bits, where each bit can have the value zero or one. In quantum computing the information is encoded in qubits. A qubit is a two-level quantum system where the two basis qubit states are usually written as $|0\rangle$ and $|1\rangle$. A qubit can be in state $|0\rangle$, state $|1\rangle$ or (unlike a classical bit) in a linear combination of both states ($\alpha|0\rangle + \beta|1\rangle$). The name of this phenomenon is superposition.

qubit quality factor

The qubit quality factor Q consists of various components and is defined as:

$$1/Q = 1/Q_i + 1/Q_d + 1/Q_c + 1/Q_m$$

- Q_i is the qubit internal quality factor (related to the qubit's internal loss mechanisms;
- Q_d is the driving ports quality factor (for qubit control signals);
- Q_c is the qubit coupling ports quality factor (for qubit couplers);
- Q_m is the qubit measurement ports quality factor (for qubit readout).

Superconducting transmon qubits can be modelled as an anharmonic (nonlinear) oscillator, the quality factor of which is defined as:

$$Q = \omega_{01}/\gamma \gg 1$$

- ω_{01} is the frequency of the qubit drive tone, i.e. the resonator microwave frequency that changes its quantum state from the ground state $|0\rangle$ to the first exited state $|1\rangle$ [21].

  $$\omega_{01} = E_1 - E_0/\hbar$$

  - E_0 is the energy level associated with the ground state $|0\rangle$;
  - E_1 is the energy level associated with the first exited state $|1\rangle$;
  - $\hbar$ (h-bar) is the reduced Planck constant, which is $h/2\pi$(the value of h is $6.62607015\times10-34$ Js).

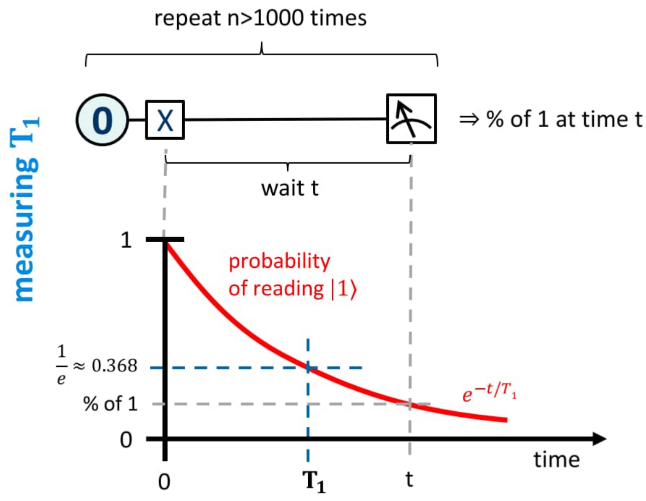
[21] Because of the transmon's anharmonicity, further excitations with the qubit's drive tone will not cause its quantum state to transit to higher exited states.

- γ is the rate of the energy dissipation caused by all sources of dissipation (internal, driving ports, coupling ports and measurement ports).

The coherence time (aka bit-flip error) T_1 is the time over which the qubit spontaneously transits from the exited state |1⟩ to the ground state |0⟩:

$T_1 = 1/\gamma = Q/\omega_{01}$

There are different sources of relaxation (aka energy dissipation) called "baths". The qubit thermalises to these "baths" in T_1 time. The qubit relaxation time is measured with a simple experiment using an X gate and measuring the result n times at different t times. T_1 corresponds to the time when the probability of obtaining a |1⟩ reaches 1/e (e = 2.718281828459045…).



T1 measurement (source: Olivier Ezratty 2023)

Even for a completely lossless resonator, the resonator frequency ω_{01} will fluctuate randomly due to some external parameters such as local magnetic or electric fields, which will cause the excitation state |1⟩ to lose phase coherence over time.

T_0 is defined as the "pure dephasing time", i.e. the time over which the qubit loses the phase information in its probability amplitudes α and β (destroying the interference between them), when assuming infinite T_1.

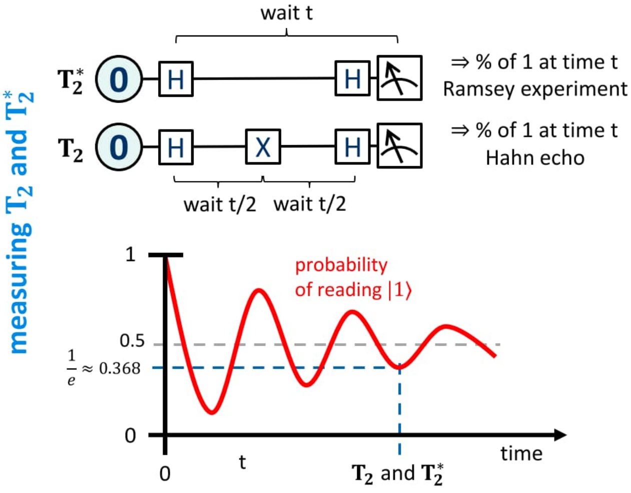
Real qubits experience damping which also causes loss of phase information. The actual dephasing time (aka phase-flip error) T_2 is defined as the time over which phase information is lost under real circumstances; it is defined as:

$1/T_2 = 1/2T_1 + 1/T_0$

In practice, two variants of qubit dephasing time measurement are being used:

1. The average phase relaxation time T_2 corresponding with the probability that the qubit's state has relaxed to |0⟩ is equal to 1/e for a qubit with Dynamical Decoupling (DD), which consists of applying echo sequences to the qubit to compensate for low frequency decoherence. T_2 (aka T_2^{echo} or T_2^{DD}) is obtained with a so called Hahn echo experiment using H and X gates.

2. The elapsed time T_2* corresponding with the probability that the qubit's state has relaxed to |0⟩ is equal to 1/e when the qubit is left to evolve freely. T_2* is obtained with a so-called Ramsey experiment using H gates.



T_2 and T_2* measurements (source: Olivier Ezratty 2023)

In general T_2* ≤ T_2 ≤ 2 T_1. T1 and T_2/T_2 * can vary widely between qubit technologies.

Note

The above description is based on the modelling of a transmon qubit as an anharmonic (nonlinear) oscillator, but the generic definitions for T_0, T_1 and T_2 are also applicable to other qubit technologies.

qubit register

In a quantum computer, qubits are organised in registers, like the bit registers in today's classical processors but not quite the same though. One key difference is that a quantum computer has only one register and not many as current classical processors.

The most important difference between a qubit register and a classical bit register is the amount of information that can be manipulated simultaneously. In classical computers, the bit registers store bitstrings, integers or floating-point numbers on which elementary logical or arithmetic operations are performed. In contrast, a register of n qubits is a vector in a 2^n dimensional space of complex numbers. These complex numbers are the amplitude of each computational quantum state and the total of their norms equals 1 since these are probabilities. Hence the dimensionality of a n-qubit register is exponentially larger than that of a n-bit register.

Rabi oscillation

Rabi oscillations, named after the American physicist Isidor Isaac Rabi, are oscillations between the quantum states of a two-level quantum system ($|0\rangle$ and $|1\rangle$ for a qubit), when it is exited at a frequency close to its resonance ω_{01}, which is defined by $\Delta E = \hbar\omega_{01}$ (ΔE is the energy difference between the ground and exited states and $\hbar$ is the reduced Planck constant).

Rapid Single Flux Quantum (RSFQ)

Rapid Single Flux Quantum (RSFQ) is a digital electronic technology that uses superconducting Josephson junctions to process digital signals. In RSFQ logic, information is stored in the form of magnetic flux quanta and transferred in the form of Single Flux Quantum (SFQ) voltage pulses.

rare-earth element

Rare-earth elements, also called rare-earth metals, rare-earth oxides or lanthanides, are nearly-indistinguishable lustrous silvery-white soft heavy metals. Scandium and yttrium are also considered rare-earth elements because they tend to occur in the same ore deposits as the lanthanides and exhibit similar chemical properties (but they have different electronic and magnetic properties).

rational number

A rational number is a number that can be expressed as the quotient or fraction *p/q* of two integers, a numerator *p* and a non-zero denominator *q*.

A rational number is a real number. The real numbers that are rational are those whose decimal expansion either terminates after a finite number of digits. A real number that is not rational is called irrational.

Irrational numbers include the square root of 2, π, e, and the golden ratio (ϕ). Since the set of rational numbers is countable, and the set of real numbers is uncountable, almost all real numbers are irrational.

real number

Real numbers can be thought of as points on an infinitely long line called the number line or real line, where the points corresponding to integers are equally spaced.

Reed-Solomon code

Reed–Solomon codes, named after the American mathematicians Irving Stoy Reed and Gustave Solomon, are a group of error-correcting codes that operate on a block of data treated as a set of finite-field elements called symbols. Reed–Solomon codes are able to detect and correct multiple symbol errors.

Resource and Performance Assessment (RPA)

Resource and Performance Assessment (RPA) refers to estimating (as accurately as possible) the resource requirements (number of qubits, number of measurements, fidelity, etc.). for achieving a given quality (target quality) of solution for a specific quantum algorithm for a specific (set of) problem instance(s).

reverse annealing

Reverse annealing uses classical simulated annealing to find a trivial solution which is then transferred to quantum annealing to find better solutions.

reversible computation

Operations used in quantum computation other than for measurement must be reversible. If an irreversible operation would be performed, information would be lost, meaning that a measurement has been performed.

Note: This requirement applies to a theoretical noiseless quantum computer. In a noisy quantum computer the qubit quantum states decohere and its gate operations can therefore not be reversed.

Rivest–Shamir–Adleman (RSA)

Rivest–Shamir–Adleman (RSA) is a public-key cryptography (aka asymmetric cryptography) algorithm that is widely used. It is was conceived by the American cryptographer and computer scientist Ronald Linn Rivest, the Israeli cryptographer Adi Shamir and the American computer scientist Leonard Adleman in 1977[22]. The security of RSA cryptography is based on the difficulty of solving the integer factorisation problem.

Rydberg atom

A Rydberg atom, named after the Swedish physicist Johannes Robert Rydberg, is an excited atom with one or more electrons that have a very high principal quantum number. The principal quantum number is a non-zero integer value which indirectly describes the size of the electron orbital. The higher this number, on average the farther away the corresponding electron is from the nucleus.

Rydberg atoms have a number of interesting properties, e.g. an exaggerated response to electric and magnetic fields, long decay periods and electron wavefunctions that approximate, under some conditions, classical orbits of electrons around the nuclei.

scalar

In linear algebra a scalar is a real number.

Schrödinger equation

The Schrödinger wave equation is a linear partial differential equation that governs the wave function of a quantum-mechanical system. It is a key result in quantum mechanics, and its discovery was a significant landmark in the development of the subject. The equation is named

[22] An equivalent system had been developed secretly at GCHQ by the British mathematician and cryptographer Clifford Cocks in 1973 (it was declassified in 1997).

after the Austrian (later naturalised Irish) physicist Erwin Rudolf Josef Alexander Schrödinger, who postulated the equation in 1925.

According to the Copenhagen interpretation of quantum mechanics, the Schrödinger wave equation is the best possible description of a quantum system. This equation gives the quantum-mechanical evolution of a massive non-relativistic quantum object as a wave function giving the probabilities of finding the quantum object at a particular position in space at a given time.

“Massive” refers to quantum objects that have mass (unlike photon particles which are massless) and “non-relativistic” refers to quantum objects whose kinetic energy is smaller than twice their rest mass energy defined by Einstein's famous equation $E=mc^2$ (this implies that the speed of these quantum objects is not close to the speed of light c).

The Schrodinger equation is not applicable to photons and relativistic massive quantum objects. The time evolution of photons is described by Maxwell’s equations and their various derivations, while the time evolution of relativistic massive quantum objects is described by the Dirac and Klein-Gordon equations.

Secure Hash Algorithm (SHA)

Secure Hash Algorithm (SHA) is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a US Federal Information Processing Standard (FIPS). SHA was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm (DSA).

The SHA family includes the following hash algorithms:

- SHA-0: the original version published in 1993. It is a 160-bit hash function which resembles Ron Rivest's MD5 algorithm. SHA-0 was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by SHA-1.
- SHA-1: a slightly revised version of SHA-1. When cryptographic weaknesses were subsequently discovered in SHA-1, the standard was no longer approved for most cryptographic uses.
- SHA-2: A family of two similar hash functions (also designed by the NSA) with different block sizes, known as SHA-256 and SHA-512. These hash functions differ in the word size: SHA-256 uses 32-bit words where SHA-512 uses 64-bit words. There are also truncated versions of each standard, known as SHA-224, SHA-384, SHA-512/224 and SHA-512/256.
- SHA-3: A hash function selected in 2012 following a public competition among organised by NIST (it was submitted under the name Keccak). SHA-3's internal structure differs significantly from the rest of the SHA family. It supports the same hash lengths as SHA-2.

security protocol

A security protocol like Transport Layer Security (TLS) describes how the encryption algorithms like AES and RSA should be used. A detailed security protocol includes details about data structures, representations and whether it can be used with interoperable versions.

set theory

The notation $x \in S$ indicates that x is an element of the set S.

The notation $A \subset B$ indicates that the set A is a subset of the set B.

The set of natural numbers is $\mathbb{N} := \{ 0, 1, 2, \dots \}$.

The set of integers is $\mathbb{Z} := \{ \dots, -2, -1, 0, 1, 2, \dots \}$.

The set of rational numbers (aka fractions) is $\mathbb{Q} := \{ p/q\colon p, q \in \mathbb{Z}, q \neq 0 \}$.

The set of real numbers is $\mathbb{R}$ and contains any number that can be approximated to any level of precision by a sequence of rational numbers.

The set of complex numbers is $\mathbb{C} := \{ a + bi\colon a, b \in \mathbb{R} \}$.

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Shor's algorithm

Shor's algorithm is a quantum algorithm for solving the integer factorisation and discrete logarithm problems. It was discovered in 1994 by the American mathematician Peter Williston Shor. Shor's algorithm runs in Polynomial time (P), meaning the time taken is polynomial in *log N*, where *N* is the size of the integer given as input. This is almost exponentially faster than the most efficient known classical factoring algorithm, the Number Field Sieve (NFS), which works in sub-exponential time.

Side-Channel Attack (SCA)

Side-Channel Attacks (SCAs) are based on information gained from the implementation of a cryptographic scheme, rather than exploiting weaknesses in the cryptographic scheme itself. Execution time, power consumption, electromagnetic emanation[23], or even heat, light, sound and

[23] Note that "electromagnetic emanation" should not be confused with ElectroMagnetic Compatibility (EMC) and ElectroMagnetic Interference (EMI), which refer to technologies and standards for avoiding interference of all kinds of

vibrations that are produced by a cryptographic system can be exploited to perform side-channel attacks. Some types of side-channel attacks require physical access to the cryptographic system or its communication facilities, while others do not. Side-channel attacks may require (in-depth) technical knowledge of the internal operation of an implementation, but so-called “black-box attacks” do not require such knowledge.

Simulated Quantum Annealing (SQA)

Simulated Quantum Annealing (SQA), aka simulated annealing, is inspired by quantum annealing. SQA mimics quantum tunnelling effects on classical computers to perform annealing through a Monte Carlo simulation, which increases the potential to find the global optima faster than traditional annealing algorithms for large-size combinatorial optimisation problems.

simulation versus emulation

Simulation is the imitation of the operation of a system over time and is based on a model which represents its key characteristics and behaviours. Simulation is used for various purposes, e.g. testing, optimising, performance tuning, etc. of technology being designed, the study of physical systems based on scientific modelling of these systems, etc.

Emulation is a technique that enables one system (the emulator) to behave (almost) exactly like another system (the target). The Church-Turing thesis implies that, in theory, any computing environment can be emulated within any other computing environment, assuming memory limitations are ignored.

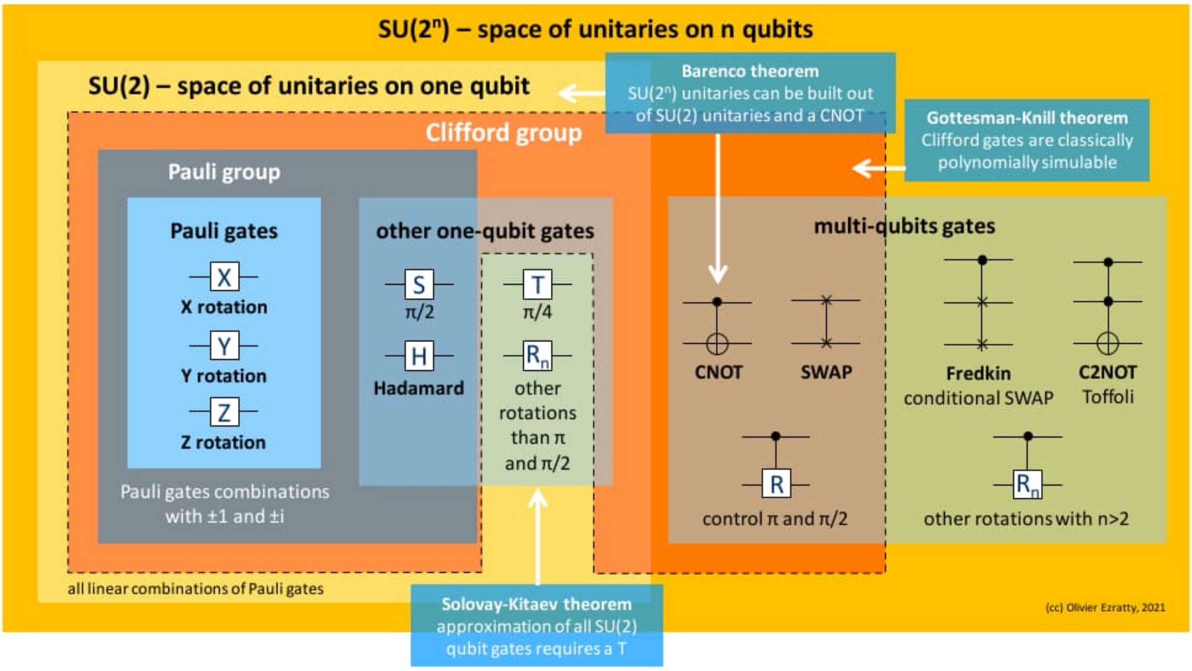
skyrmion

The skyrmion, named after the British physicist Tony Hilton Royle Skyrme, is a topological quasiparticle which has the remarkable property of being able to model, with reasonable accuracy, multiple low-energy properties of the nucleus of an atom, simply by fixing its radius.

equipment with one another and with regulated radio waves such as broadcast radio/TV signals, mobile network radio signals, GPS signals, etc.

Special Unitary (SU)

The Special Unitary group SU (2^n) is the space of unitary transformations applicable on n qubits. It covers all the unitary transformations that can be performed on n qubits (quantum gates are unitary, because they are implemented via the action of a Hamiltonian for a specific time, which gives a unitary time evolution according to the Schrödinger equation). Hence SU(2) denotes the unitary transformations applicable to a single qubit, SU(4) denotes the unitary transformations applicable to 2 qubits, and so on.



SU(2ⁿ) – space of unitaries on n qubits
SU(2) – space of unitaries on one qubit
Barenco theorem
SU(2ⁿ) unitaries can be built out of SU(2) unitaries and a CNOT
Gottesman-Knill theorem
Clifford gates are classically polynomially simulable
Clifford group
Pauli group
Pauli gates
X
X rotation
Y
Y rotation
Z
Z rotation
Pauli gates combinations with ±1 and ±i
other one-qubit gates
S
π/2
H
Hadamard
T
π/4
Rn
other rotations than π and π/2
multi-qubits gates
CNOT
SWAP
Fredkin
conditional SWAP
C2NOT
Toffoli
R
control π and π/2
Rn
other rotations with n>2
all linear combinations of Pauli gates
Solovay-Kitaev theorem
approximation of all SU(2) qubit gates requires a T
(cc) Olivier Ezratty, 2021

spin

In classical physics, charged spinning objects have magnetic properties. When certain subatomic particles move through a magnetic field, they are deflected in a manner that suggests they are also spinning. However, this analogy is misleading and would lead to paradoxes. For instance, unlike a spinning classical object, the spin of an electron never changes, and it has only two possible orientations. Furthermore, the very notion that subatomic particles are "solid objects" that can rotate in space contradicts the laws of quantum mechanics. The term "spin", however, is still being used in quantum mechanics. The spin concept was introduced by the Austrian theoretical physicist Wolfgang Ernst Pauli, who also proved the spin–statistics theorem, which states that bosons have integer spin and fermions have half-integer spin.

Spontaneous Parametric Down-Conversion (SPDC)

Spontaneous Parametric Down-Conversion (SPDC) converts high-energy photons into pairs of photons of lower energy, based on pumping nonlinear optical waveguides (crystals) or cavities. It can be used to create pairs of entangled photons as well as single photons.

state vector

The physical state of a quantum system is represented by a symbol $| \rangle$ known as a ket (Dirac notation) and it is referred to as a (quantum) state vector or just (quantum) state.

superconducting qubit

Superconducting qubits are engineered “miniature” quantum systems, which are for example based on superconducting current loops or superconducting nanowires.

superconductivity

Superconductivity relates to the ability of some materials to conduct electricity without resistance[24]. It generally occurs at very low temperatures and is linked to the behaviour of electrons in some crystalline structures who happen to gather in pairs (called Cooper pairs) who become bosons and exhibit a collective behaviour enabling them to freely move around within the crystalline structure.

About 50 chemical elements are superconducting at low temperatures, but their superconductivity temperatures and pressure threshold are very variable. The superconducting effect is at its maximum for atoms that have a large number of valence electrons (i.e. electrons in the last orbital). Metals that are superconductors are generally poor conductors in their normal state, while most good conductors like copper, gold and silver are not superconductors. Superconductivity is also possible with composite alloys. The most common superconducting materials are aluminium and a niobium and titanium alloy, as used in superconducting wires in MRI imaging systems and in superconducting qubit technology.

[24] Superconductivity was discovered experimentally in 1911 by the Dutch physcists Heike Kamerlingh Onnes, Cornelis Dorsman, Gerrit Jan Flim and Gilles Holst at the University of Leiden.

superdense coding

Superdense coding (aka dense coding) is a quantum communication protocol mechanism to communicate a number of classical bits of information by only transmitting a smaller number of qubits, under the assumption of sender and receiver pre-sharing an entangled resource.

supersingular elliptic curve

Instead of defining operations that map points on an elliptic curve, it is possible to define operations to map an elliptic curve onto another elliptic curve. If such a mapping exhibits certain specific properties, it is called an isogeny ("isogeny" has its origins in the Greek language and means "equal in kind or nature"). Cryptographic schemes that use isogenies between ordinary elliptic curves are not quantum-resistant but cryptographic schemes that use isogenies between supersingular elliptic curves (elliptic curves that have a special structure) can be made quantum-resistant.

Support-Vector Machine (SVM)

Support-Vector Machines (SVMs) are supervised Machine Learning (ML) models with associated learning algorithms that analyse data for classification and regression analysis. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier.

surface code

A surface code is a type of Quantum Error Correction (QEC) code that is tolerant to relatively high qubit error rates. Surface codes require a large number of physical qubits per logical qubit and have a design constraint in that physical qubits must be connected to their immediate neighbours in a 2D structure.

SWAP gate

A SWAP gate is a quantum gate that inverts the state of two qubits. It is very useful since the qubit geometries of most quantum computers do not provide for any-to-any qubit connectivity. In this case, SWAP gates can be used to set up the qubit connectivity required by a specific quantum algorithm.

symmetric cryptography

Symmetric cryptography uses a single cryptographic key (known as the ”secret key”) for both the encryption of plaintext and the decryption of the corresponding ciphertext[25].

Symmetric encryption algorithms are categorised into block and stream ciphers:

- Block ciphers convert data in plaintext into ciphertext in fixed-size blocks. The block size generally depends on the encryption scheme. If the plaintext length is not a multiple of the block size the encryption scheme uses padding to ensure complete blocks are encrypted.

- Stream ciphers encrypt a continuous string of binary digits by applying time-varying transformations on plaintext data. Therefore, this type of encryption works bit-by-bit, using keystreams to generate ciphertext for arbitrary lengths of plaintext messages. Stream encryption ciphers achieve this using feedback shift registers to generate a unique nonce (number used only once) to create the keystream.

tensor

A tensor is an algebraic object that describes a multilinear (multidimensional) relationship between sets of algebraic objects related to a vector space. Tensors may map between different objects such as scalars (a scalar is a tensor of order 0), vectors (a vector is a tensor of order 1), matrices (a matrix is a tensor of order 3), and tensors of order 3 and higher.

In quantum computing, tensors are typically used to describe the state of qubit registers. A qubit is represented by a vector of two complex numbers. A register of *n* qubits is represented by an *n* x *2* matrix with resulting from the tensor product of *n* vectors of *2* complex numbers. The tensor product represents the combinatorial space of the values that a combination of qubits can take before entanglement comes into play and creates non separable vector states, i.e. which cannot be expressed as tensor products of individual quantum states.

[25] For some algorithms, the key value used for decryption is derived from the key value used for encryption by a simple transformation.

tensor network

Tensor networks aka tensor network states are a class of variational wave functions used in the study of many-body quantum systems. Tensor networks extend one-dimensional matrix product states to higher dimensions while preserving some of their useful mathematical properties.

Toffoli gate

A Toffoli gate[26], named after the Italian-American scientist Tommaso Toffoli, is a quantum gate operating on three qubits which modifies the value of the third qubit if the value of the first two is 1. It is also called CCNOT or C2NOT gate.

tomography

Tomography is the reconstruction of a comprehensive model (of something) from many partial cross-sections or slices, each of which provides only a limited view that may be useless by itself.

topological quantum computing

Designing anyons based on a mix of conventional and superconducting electronics is currently an active area of research quantum in the field of computing technology. For example, Microsoft has made substantial investments in the quest for developing Majorana qubits.

The most distinctive advantage of such “designed anyons”[27] is their potential noise immunity. The worldlines[28] of two particles can wind around one another in a 3-dimensional spacetime consisting of one temporal dimension and two spatial dimensions. In the case of more than two particles, worldlines can become interwoven in elaborate patterns called braids. There are different topological classes of braids, distinguished among other things by the number of times different strands wind around one another. The wave functions of these multiparticle quantum objects store memories of the braids formed by their worldlines and the transformation of the state of the quantum system depends only on the overall form (i.e. topological class) of these worldlines. The information which is stored in the state of such quantum systems is therefore

[26] Not to be confused with a T gate!

[27] Not to be confused with anyons based on the natural state of matter.

[28] The worldline of an object is the path that an object traces in space-time; it is an important concept in theoretical physics.

impervious to small errors as the braids retain their overall form (topology) even if they are jostled a bit. This particular property could possibly enable the development of inherently reliable physical qubits and might reduce and possibly even eliminate the overhead of performing explicit Quantum Error Correction (QEC).

transmon qubit

A transmission-line shunted plasma oscillation (transmon) qubit is a superconducting qubit based on a superconducting current oscillating at two different frequencies across a Josephson junction.

transpilation

A transpiler, aka transcompiler, source-to-source compiler or source-to-source translator, is a type of translator that takes the source code of a program written in a programming language as its input and produces an equivalent source code in the same or a different programming language. A transpiler translator converts between programming languages that operate at approximately the same level of abstraction, while a traditional compiler translates from a higher level programming language to a lower level programming language.

trapped-ion qubit

An ion trap is a combination of electric and/or magnetic fields used to capture charged particles (known as ions), often in a system isolated from an external environment. In comparison to neutral atom traps, ion traps have deeper trapping potentials (up to several electronvolts) that do not depend on the internal electronic structure of a trapped ion. This makes ion traps more suitable for the study of light interactions with single atomic systems.

Traveling Salesman Problem (TSP)

The Traveling Salesman Problem (TSP) asks the following question: given a list of cities and the distances between each pair of cities, what is the shortest possible route that visits each city exactly once and returns to the origin city? It is an NP-hard problem in combinatorial optimisation. In computational complexity, the decision version of the TSP, where given a length L, the task is to decide whether the graph has a tour of at most L, belongs to the class of NP-complete problems.

trotterization

Trotterization is a technique used in quantum computing which breaks down the evolution of a quantum system into a series of smaller timesteps.

Twin-Field QKD (TF-QKD)

Twin-Field QKD (TF-QKD) technology is similar to MDI-QKD technology, but is designed to generate secret key bits from single-photon interference in the intermediate node, thus removing the need to remedy photon losses via sophisticated techniques.

universal gate set

A universal quantum gate set is set of quantum gates that allows us to (approximately) emulate any given set of quantum gates. It is a group of quantum gates that has the property of allowing the creation of all unitary operations on qubits. From a practical point of view, it also allows to create all known quantum gates for one, two and three qubits. Such a quantum gate set must be able to create superpositions and entanglement, and it must contain at least one quantum gate with no real parameters, i.e. complex numbers instead of real numbers.

Some examples of universal quantum gate sets:

- CNOT gate + all single-qubit gates (Barenco theorem);
- Toffoli gate paired with a computational basis changing operator with real coefficients (such as for example the H gate);
- CNOT gate + 1/8 turn T gate + H gate or CNOT gate + S gate + H gate, using approximations with a maximum error rate ϵ (Solovay-Kitaev theorem).

Universal Hash Function (UHF)

Universal hashing refers to selecting a hash function at random from a family of hash functions with a certain mathematical property, which guarantees a low number of collisions in expectation, even if the data is chosen by an adversary. Many Universal Hash Function (UHF) families are known for hashing integers, vectors and strings; their evaluation is often very efficient.

Variational Quantum Algorithm (VQA)

A Variational Quantum Algorithm (VQA) is a hybrid quantum-classical optimisation algorithm in which an objective function (usually encoded by a parameterised quantum circuit) is evaluated by quantum computation, and the parameters of this function are updated using classical optimisation methods.

Variational Quantum Eigensolver (VQE)

The Variational Quantum Eigensolver (VQE) is a type of hybrid quantum-classical Variational Quantum Algorithm (VQA) algorithm that uses the variational principle to compute the ground state energy of a Hamiltonian, a problem that is central to quantum chemistry and condensed matter physics.

Variational Quantum Factoring (VQF)

Variational Quantum Factoring (VQF) is an alternative to Shor's quantum algorithm, which employs techniques to map the factoring problem to the ground state of an Ising Hamiltonian.

vector

A vector is a quantity that has both magnitude and direction. It is typically represented by an arrow whose direction is the same as that of the quantity and whose length is proportional to the quantity's magnitude. Although a vector has magnitude and direction, it does not have position.

A vector can also be seen as a two-dimensional array of scalar elements.

Vectors can be multiplied by scalars (scalar multiplication), they can be added together (vector addition), they can be subtracted from each other (vector subtraction) and they can be multiplied with each other. Vector multiplication is not uniquely defined as different types of products can be defined for pairs of vectors, including:

- the *inner product* (aka dot product or scalar product) of two vectors u and v of the same dimension n (denoted by u^Tv or $u.v$) is a single number that is the sum of the products u_iv_i (i ∈ {1, … , n}) of the corresponding elements of the two source vectors;
- the *outer product* (aka tensor product) of two vectors u and v of dimensions n and m (denoted by uv^T or $u \otimes v$) is an n × m matrix, which consists of n rows that are obtained by

multiplying each element u_i (i ∈ {1, … , n}) of the first vector by each element v_j (j ∈ {1, … , m}) of the second vector.

vector space

A vector space over a field *F* (often the field of the real numbers) is a set *V* equipped with two binary operations satisfying the axioms listed below. Elements of *V* are called vectors, and elements of *F* are called scalars. The first operation, vector addition, takes any two vectors *v* and *w* and outputs a third vector $v + w$. The second operation, scalar multiplication, takes any scalar *a* and any vector *v* and outputs a new vector *av*.

The axioms that addition and scalar multiplication must satisfy are the following.

- associativity of addition: $u + (v + w) = (u + v) + w$
- commutativity of addition: $u + v = v + u$
- identity element of addition: there exists an element *0* in *V*, called the zero vector (or simply zero), such that $v + 0 = v$ for all *v* in *V*
- inverse elements of addition: for every *v* in *V*, there exists an element $-v$ in *V*, called the additive inverse of *v*, such that $v + (-v) = 0$

  (the first four axioms mean that *V* is an abelian group under addition)
- distributivity of scalar multiplication with respect to vector addition: $a(u + v) = au + av$
- distributivity of scalar multiplication with respect to field addition: $(a + b)v = av + bv$
- compatibility of scalar multiplication with field multiplication: $a(bv) = (ab)v$
- identity element of scalar multiplication: $1v = v$, where *1* denotes the multiplicative identity of *F*

An element of a specific vector space could be a sequence, a function, a polynomial or a matrix. Linear algebra is concerned with those properties of such objects that are common to all vector spaces.

Von Neumann architecture

The Von Neumann architecture is a computer architecture based on a 1945 description by the Hungarian-American mathematician and physicist John von Neumann and others. It describes a design architecture for a digital computer system with the following components: a processing unit that contains an arithmetic logic unit and processor registers, a control unit that contains an instruction register and program counter, memory that stores data and instructions, external mass storage and input and output mechanisms.

The term has evolved to mean any stored-program computer system in which an instruction fetch and a data operation cannot occur at the same time because they share a common bus. This is referred to as the Von Neumann bottleneck and often limits the performance of such a computer system.

wave packet

A wave packet is a burst of an electromagnetic wave that travels as a unit. It is found by the addition of an infinite number of sinusoidal waves of different frequencies, phases and amplitudes creating constructive and destructive interferences in a small region in space, and destructively elsewhere.

Wegman-Carter Authentication (WCA)

Wegman-Carter Authentication (WCA) message authentication, named after the American computer scientists Mark N. Wegman and J. Lawrence Carter, is based on secretly selecting a hash function (using a salt) from a library of Universal Hash Functions (UHFs) and sending its output to a Pseudo-Random Function (PRF), to create a Message Authentication Code (MAC). The WCA scheme is information-theoretically secure (i.e. secure against adversaries with unlimited computing and storage capabilities), provided that the authentication key is uniformly distributed.

worldline

The worldline of an object is the path that an object traces in space-time; it is an important concept in theoretical physics.

XOR

The eXclusive OR (XOR), or exclusive disjunction, is a logical operation that is true if and only if its arguments differ (i.e. one is true and the other is false).

Zero-Knowledge Proof (ZKP)

A Zero-Knowledge Proof (ZKP) is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, while the prover avoids conveying any additional information apart from the fact that the statement is indeed true. The essence of ZKPs is that it is trivial to prove that one possesses knowledge of certain information (e.g. by simply revealing it); the challenge is of ZKP to prove such possession without revealing the information itself or any additional information about it. In practice, most zero-knowledge proofs are based on the following three-step mechanism:

1. the prover generates some random value (the commitment) and sends it to the verifier;

2. the verifier responds with a challenge value generated uniformly at random;

3. the prover computes the final proof based on both the commitment and challenge.