Quantum Engineering
Centre for Doctoral Training

Cohort III*

Quantum at Home

Domestic Applications of Emerging Quantum Technologies

Atkinson G., Chadwick R., Diniz J., Dixon W.,
Eftaxias N., Flynn B., Ibberson D., Koteva K., Lennon J.,
Monroy-Ruz J., Wakefield R., Wilson M.

University of Bristol

August 2017

*Email: quantum-at-home@bristol.ac.uk

Abstract

Physical devices designed to exploit the counterintuitive phenomena that quantum mechanics describes promise to supersede some of the current technologies in fields as diverse as computing, communication, health, science, navigation, security, imaging, entertainment and sensing. Here we explore the potential applications of quantum technologies that may affect our day-to-day lives by detailing the near-term realisations and some more speculative ideas. It is clearly demonstrated that quantum technologies will influence society in many different ways and that quantum technologies may replace current technologies, and in some cases offer completely novel applications. This work informed the development of the website www.quantumathome.co.uk.

Contents

List of Figures

Acronyms

ANN Artificial Neural Network.

AQS Analog Quantum Simulation.

ATM Automated Teller Machine.

BBBW Bennet, Brassard, Breidbart and Wiesner.

BEC Bose Einstein Condensate.

BQC Blind Quantum Computation.

CAP/DPA Chip Authentication Program/Dynamic Passcode Authentication.

COW Coherent One Way.

CPU Central Processing Unit.

DAC Digital-to-Analog Converter.

DI Device Independent.

DQS Digital Quantum Simulation.

EEG Electroencephalography.

EFTPOS Electronic Funds Transfer at Point of Sale.

FRET Fluorescence Resonance Energy Transfer.

GDP Gross Domestic Product.

GPS Global Positioning System.

GPU Graphics Processing Unit.

IEEE Institute of Electrical and Electronics Engineers.

iTAN indexed Transaction Authentication Number.

KNN K-Nearest Neighbour.

LAN Local Area Network.

LDA Linear Discriminant Analysis.

LEDs Light Emitting Diodes.

MEG Magnetoencephalography.

MEMS Microelectromechanical Systems.

MRI Magnetic Resonance Imaging.

NMF Non-negative Matrix Factorisation.

NV Nitrogen Vacancy.

OECD Organisation for Economic Co-operation and Development.

OFDM Orthogonal Frequency Division Multiplexing.

PCA Principal Component Analysis.

QC Quantum Computing.

QD Quantum Dot.

QDB3 Quantum Dot Blinking with 3D Imaging.

QGS Quantum Gravity Sensor.

QHE Quantum Heat Engine.

QHL Quantum Hamiltonian Learning.

QKD Quantum Key Distribution.

QML Quantum Machine Learning.

QND Quantum Non-Demolition.

QPU Quantum Processing Unit.

QRNG Quantum Random Number Generator.

RAM Random Access Memory.

RANSAC RANdom SAmple Consensus voting scheme.

RNG Random Number Generator.

SOFI Super-resolution Optical Fluctuation Imaging.

SQUID Superconducting Quantum Interference Device.

STED Stimulated Emission Depletion.

STORM STochastic Optical Reconstruction Microscopy.

SVM Support Vector Machine.

UV Ultraviolet.

VQ Vector Quantisation.

WEF World Economic Forum.

WEP Wired Equivalent Privacy.

WPA Wi-Fi Protected Access.

1 Introduction

Myriad technologies developed from advances in quantum mechanics in the 20th century are now fundamental parts of society. Most notably, an understanding of semiconductor physics led to the development of the microprocessor. Today, another wave of quantum technologies are in development. These technologies tend to exploit entanglement, a more subtle aspect of quantum mechanics, where two systems are correlated in such a way that their states cannot be described independently.

Around the world there are initiatives driving forward quantum technologies, which in the field of quantum computation has been likened to an arms race [1]. In China, the 2016–2020 5-year plan lists quantum communications and computing as one of five top priorities for development [2]. In the US, though government investment in science is dropping [3], commercial enterprises, such as IBM, Google and Microsoft, remain world leaders in Quantum Computing (QC) technologies, and there are government bodies still with a strong interest in QC, most notably in defence and intelligence [4].

Flagship projects in the UK (£270 million [5]) and the EU (€1 billion [6]) are comparable to the other grand scientific projects of the 21st century: mapping the human brain, graphene and fusion. Globally in 2015, there were over 7000 researchers in quantum technologies with an annual expenditure of $1.5 billion [7].

The purpose of this document is to explore quantum technologies, their potential advantages over current technology and where their adoption might impact our lives. All included research is under the umbrella of the latest revolution in quantum technologies, and as such most primarily replace an inherently classical technology. There are areas where the distinction is harder to make. Quantum technologies are defined as technologies which: exploit quantum phenomena, notably superposition and entanglement or the coherent control of quantum states; are novel, that is they are not new iterations of older technologies which use quantum effects; and finally offer some advantage over competitors.

Sections 2 - 7 of this document are a summary of the quantum technologies explored and their applications in the fields Health, Security, Environment and Entertainment. Following this summary are 15 Articles on quantum technologies covering current technology, the advances in quantum technologies, the improvement they may realise and their application.

2 Health

In the UK, expenditure on health is rising as a proportion of Gross Domestic Product (GDP) [8]. In developed economies, population demographics are getting older [9], new drugs are becoming more costly to develop and trial [10], and life-span is extending. A report by the Organisation for Economic Co-operation and Development (OECD) in 2015 found “Healthcare costs are rising so fast

in advanced economies that they will become unaffordable by mid-century without reforms" [11]. Here, healthcare is defined as the tools for diagnosis and treatment of disease. Quantum technologies show some promise for decreasing the cost and size, and increasing the efficacy of these tools.

The power of quantum computation to simulate quantum systems was proposed by Feynmann [12] and could end up having a significant and meaningful impact in the development of new drugs. Even the largest and most advanced classical computers cannot simulate the state of small molecules. With the advent of rudimentary quantum computation devices, simulations that are otherwise intractable will become possible (Article A), and quantum adiabatic optimisers for looking into protein folding could open up new paradigms of medical research and reduce the cost of complex drug research by simulating complex systems before starting expensive and potentially harmful trial processes.

Further, imaging and sensing are fundamental tools used in healthcare for the detection of disease. Advances in imaging of the human body (skeletal structure, biological systems and the brain) promise to improve on the sensitivity of current devices, increase the mobility and stability, and decrease the cost, even to the extent that currently prohibitively expensive devices, such as MRI machines, could be used in houses (Article B).

Finally, quantum enhanced cameras, by exceeding the classical diffraction limit, can offer lower cost methods to image microscopic biological structures with more resolution than is available in current optical imaging devices (Article C), and the application of Quantum Dot (QD) technology may be less prohibitively complex than current fluorescence technology in the field of biological and chemical sensing (Article D).

3 Security

Society is spending more time in digital spaces, with the average adult spending 5.6 hours using digital media per day in 2016 [13]. The compromise between privacy and security is one of the big ethical debates of the 21st century [14], and in a survey conducted by Pew Research Centre in 2013, 86% of respondents claimed to have taken steps to avoid surveillance online [15].

Advances in Quantum Key Distribution (QKD), in systems that are already commercially available, hold potential promise for secure and future-proof key distribution between two parties, with early adopters in defence and commerce. Further developments in these technologies open the potential for application in a range of fields and lower cost implementation. Most notably, satellite-to-ground demonstrations and systems integrated on silicon are significant advances and potential applications include backbone networks (Article E), and handheld authenticators (Article F).

With access to quantum channels, each home may be securely connected to a quantum processing unit where data can be processed and returned with no possibility of an observer learning anything about the data in blind quantum computation (Article G).

Further, the intrinsic and true randomness of quantum systems can be used in random number generation. A Quantum Random Number Generator (QRNG) could be certifiable, private and device independent, with applications in cryptography (Article H). Quantum research may even influence the certification of money and the development of cryptographic currencies (Article I). And finally, quantum machine learning, on early stage devices, has been demonstrated as competitive with some classical algorithms, for example in security for applications such as facial recognition (Article J).

4 Environment

It may be argued that the most difficult and potentially damaging challenge of the 21st century will be climate change. In 2017 the World Economic Forum (WEF) Global Risk Report listed the changing climate as the second Top 5 trend that will determine global development [16]. The recently signed Paris climate accord is an example of improving political will and public opinion [17]. Parallel to these policy steps, technology is being used to tackle the problems of pollution and over-consumption, specifically, though not limited to, in the fields of battery technology and solar energy: in 2015 the cost of batteries was predicted to decrease by a half in four years [18] and in 2016 the WEF found that the cost of introducing new solar capacity was the same cost or cheaper than for fossil fuels [19].

These revolutions will change the way we use and distribute power. In the field of solar energy, theoretical proposals for two channel quantum heat engines will potentially be more efficient than classical systems. A proposed system for the implementation of this is quantum dots. Additionally, quantum dots more efficiently collect solar energy than classical systems due to multiple exciton generation (Article K). Furthermore, there are theoretical suggestions for quantum interpretations of information and energy that might be applied in batteries, where it was proposed that nonclassical correlations could improve efficiency (Article L).

For locating resources, detecting sinkholes, climate research, geology and construction, advances in quantum gravity sensors may soon exceed their classical counterparts in cost, sensitivity and mobility (Article M).

5 Entertainment

Developments in technology and entertainment are linked: the television (cathode ray) and computers (microprocessor) are clear examples of this. A report by bcc research predicted that digital home entertainment systems market will reach $176.3 billion in size by 2018 [20].

In the era of big data, recommendation systems are playing a central role in the personalisation of an individuals interface with digital media [21]. Recommender systems powered by Grover's

search algorithm could improve the speed and accuracy of these systems (Article N). The example application of quantum algorithms and processors in gaming is explored in (Article O).

As discussed in Section 3, QRNGs offer true randomness, which could easily be applied as the basis of fair and verifiably random online gambling (Article H).

The shift in entertainment to the digital space (augmented reality and advancing human computer interface) will open new ways to interact with computers and entertain ourselves. Examples include brain computer interfaces (Article B).

6 Conclusion

In conclusion, there are a wealth of applications for quantum technologies, many of which have demonstrated or theorised advantage over classical or current technologies. It has been demonstrated here that these technologies will be used in the home, and people will interact with these devices directly or indirectly in their day-to-day lives.

Acknowledgements

This work was conducted by the Quantum Engineering CDT 2016/2017 cohort, University of Bristol. Funding provided by Engineering and Physical Sciences Research Council (EPSRC), and the support of the Quantum Engineering Centre for Doctoral Training and Bristol University are acknowledged.

Articles on Quantum Technologies

A Quantum Simulation

Computer simulations are programs, based on mathematical descriptions or models, which mimic the dynamic behaviour of one real system as it interacts with another. This makes them a cheap and easy way to predict the outcomes of experiments requiring conditions which cannot be safely or easily created in real life. Thus simulations have been an invaluable tool in scientific research for almost as long as computers have been around.

From investigating fundamental physics phenomena to designing the newest pharmaceutical drug, computer simulations have improved many aspects of our lives. Still, most simulations are built upon simplified models which capture only essential features of the actual physical systems and experimental data is needed to check the consistence of their predictions with real life. In order to get the most realistic results, programs which simulate the underlying physics phenomena are needed. However, predicting the behaviour of large systems at the quantum level is known to be intractable for classical computers since the resources required scale exponentially with the system size [12].

A solution to the problem above was first suggested by Richard Feynman who famously said: "Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy." [22]. Almost four decades later research into quantum simulations is more promising than ever due to recent developments in quantum computers. These are computers which would be capable of storing an exponential amount of information without taking up an exponential amount of physical resources. Different techniques of manipulating them could lead to the next generation of computer simulators.

A.1 Classical

The main problem with classically simulating quantum systems is the amount of memory required to store all parameters needed to characterise a quantum state. To begin with, a classical computer has to keep track of all the possible classical configurations of a system together with their probability amplitudes. Then, in order to describe any kind of change, like natural evolution or interaction with another system, it also has to record the operators acting on each of these configurations. Both of these actions scale exponentially with the number of particles or degrees of freedom which is why even modern supercomputers would struggle to simulate large quantum systems.

A.1.1 Monte Carlo Simulations

Introducing stochastic techniques into simulations was thought to provide a way around the exponentiality problem since they allowed statistical analysis of distributions which cannot be determined

precisely. Probably the most famous classical simulations of this type are based on Monte Carlo algorithms [23].

The core principle of these algorithms is to approximate any integral of a function by evaluating it at a relatively small set of carefully chosen points so that the final answer is considered close to the real one for the purposes of the calculation. This is a very powerful tool because it helps the evaluation of many-body functions' integrals in phase space within polynomial time of the size of the system.

However, it only works for functions which vary slowly within their parameter space and generally do not change sign as any sudden large deviations result in statistical error. In fact, one such error when sampling a non-positive semidefinite function is growing exponentially with the system size so that it completely removes any benefits that the Monte Carlo method provides. This is also known as the sign problem [24].

Unfortunately most systems experience this sort of chaotic behaviour at the quantum level which makes them impossible to simulate numerically.

Other classical simulation techniques exist like many-body perturbation theory or mean-field theories [25]. However, most of them suffer from similar to Monte Carlo methods' problems which ultimately prevents them from successfully simulating quantum physics.

A.2 Quantum

A quantum simulator is a controllable quantum system which is used to emulate another quantum system [26]. Schematics of how this works can be seen in figure A.1. Depending on the level of control and capabilities of the simulator, there are two types of simulation: analog and digital.

A.2.1 Analog Quantum Simulations

Analog Quantum Simulation (AQS) is a type of quantum simulation which does not require complete control over the simulator. This is possible when there exists a direct mapping, f, between the Hamiltonians of the two systems, H_{sys} and H_{sim}, such that [28]:

$$f : H_{sys} \to H_{sim}$$
$$f^{-1} : H_{sim} \to H_{sys}.$$

This map is chosen according to the capabilities of the AQS and the property under investigation. The advantage is that the simulator can reproduce a specific feature of the system, like the dynamics or the ground state, without simulating every aspect of it. So AQS acts as a simplified controllable model and therefore it can simulate properties of systems with higher complexity than

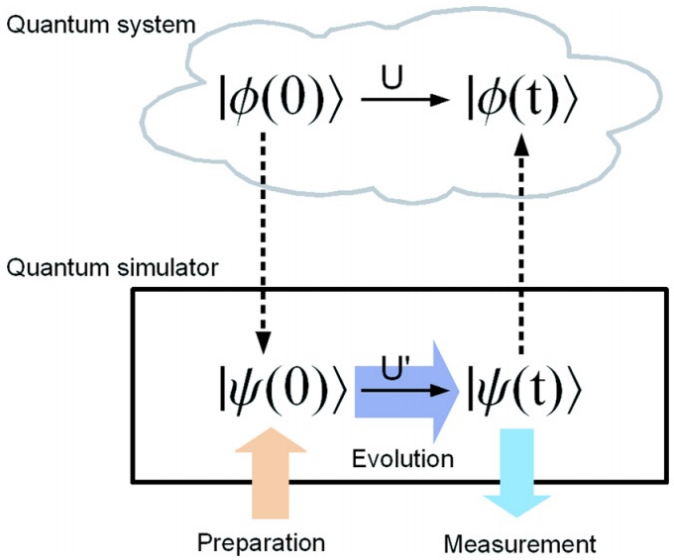


Figure A.1: Schematic representation of quantum simulation. The quantum state $|\phi(0)\rangle$ evolves to $|\phi(t)\rangle$ within the original system. The quantum simulator evolves from state $|\psi(0)\rangle$ to state $|\psi(t)\rangle$. The simulator is designed so that the following mappings exist: $|\phi(0)\rangle \leftrightarrow |\psi(0)\rangle$, $|\phi(t)\rangle \leftrightarrow |\psi(t)\rangle$ and $U \leftrightarrow U'$ where U and U' are unitary transformations. The main point of quantum simulation is that while the original system may not be controllable or experimentally accessible, the state of the simulator is. The coloured arrows indicate the controllable operations, specifically initial state preparation, engineering of evolution and final state measurement. The solid black arrows denote time evolution and the dashed arrows show the corresponding mappings. Image taken from [27].

itself. Furthermore, analog simulators are resistant to errors within limits since small uncertainties in control parameters do not affect the outcome of interest. Therefore they are particularly useful for qualitative analysis of physical conditions, like whether or not a given phase transition occurs.

Powerful, yet not requiring a universal quantum computer, AQS is considered by many experts to be the first quantum technology to change our lives.

A.2.2 Digital Quantum Simulations

In Digital Quantum Simulation (DQS), all information is encoded using superpositions of binary bit strings. For example, a particle with a half spin-up state is encoded in the qubit state $|1\rangle$, while a half spin-down particle is encoded in $|0\rangle$. Then any evolution of the system is simulated by applying different combinations of single- and two-qubit gates representing the many-qubit unitary transformation corresponding to the desired evolution. This is all possible due to the circuit model for quantum computation [29]. An example of how this scheme works can be seen in figure A.2.

The main advantage of DQS is that it is universal, i.e. any operation can be written as a combination of quantum gates and therefore can in theory be simulated on a quantum computer [31]. In practice, some operations cannot be simulated efficiently so the problem seems to remain. However, it turns out that all finite-dimensional local Hamiltonians can be simulated efficiently which is important since there exist mappings between them and most physical systems. Hence, DQS can indeed be

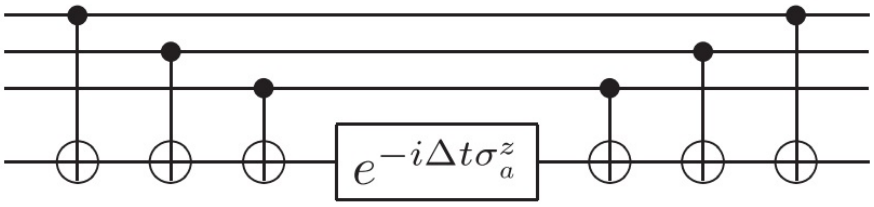


Figure A.2: A quantum circuit containing six CNOT gates and utilising a fourth, ancilla qubit (bottom line), simulates the three-body Hamiltonian $H = \sigma_1^z \otimes \sigma_2^z \sigma_3^z$. Image taken from [30]

used to simulate almost any real system as soon as a universal quantum computer is built.

A.2.3 Quantum Hamiltonian Learning

Another way to improve simulations is to introduce quantum enhanced machine learning called Quantum Hamiltonian Learning (QHL). It is based on learning the Hamiltonian of one quantum system by interfacing it with another one through a classical channel and using Bayesian interference to correlate their characteristics. This is a powerful tool because it allows the validation or rejection of current underlying physical models or their possible correction to fit the phenomena better. So far this technique has been used with a silicon-photonics quantum simulator to learn a salient Hamiltonian parameter of an electron spin in a diamond nitrogen–vacancy centre and show potential weaknesses of the current Hamiltonian model. This was developed using DQS but slight adjustments can make QHL compatible with AQS too [32].

A.3 Discussion

Quantum simulations have the potential to improve many areas of research in science and even everyday life. Better electronics and new pharmaceutical drugs are two large areas where major impact is expected.

A.3.1 Electronics

Learning more about fundamental physics phenomena can help shed light on some of the processes involved in the fabrication of advanced electronics. For example, high-temperature superconductivity is still not well understood, so various models are being developed and tested in order to find out more about it. One such model that could be simulated with an AQS is the t-J model which describes strongly correlated fermions on a lattice [33]. Here t stands for the amount of kinetic energy of a hole disrupting an antiferromagnet with interaction energy between neighbouring spins, J. Another option is to simulate copper-oxide planes in high-T superconductors by mapping them to an array of electrostatically defined quantum dots [34].

Apart from investigating the properties of existing materials, scientists are also trying to engineer new materials which could be used to build superior electronics in terms of price and capabilities. Such structures are constructed by periodically arranging mesoscopic building blocks and are called metamaterials. Their behaviour in the quantum regime can be mimicked by a quantum simulation of materials composed of regular atomic structures [35]. Developing these systems would allow precise control over the propagation of electromagnetic fields unachievable by standard materials.

A.3.2 Drugs and medicine

Simulating chemical and biological processes is more difficult than physical ones due to the scale and increased complexity involved. Yet, many algorithms and experiments have shown that progress in this area is possible. One example involves calculating the thermal rate constant using a DQS initialised to contain an equal superposition of position eigenstates which is followed by a unitary evolution made possible by the quantum Fourier transform. A sequence of measurements ends this process producing an efficient estimation of the energy spectrum and eigenstates [36].

Quantum machines could also be used to simulate the dynamics of chemical reactions in polynomial time [37]. For example, a photonic DQS has been used to calculate the energies of the hydrogen molecule [38]. Chemical reaction dynamics have also been recently investigated by nuclear spin DQS [39].

Meanwhile, AQS has been applied to one of the major challenges in modern day biology: modelling protein folding. In particular, it is used to solve the classical lattice folding optimisation problem where the sequence of amino acids held together by peptide bonds are represented by beads connected by strings within a two- or three-dimensional lattice. Then the folding of the protein is simulated by performing a self-avoiding random walk on this lattice which minimises the interaction energies between the amino acids [40]. So far small protein folding problem simulations have been successfully performed on superconducting qubits [41]. Knowledge of protein folding is expected to change our understanding of complex biological systems and allow the design of new, more powerful drugs.

B Magnetic Sensors

Many forms of medical imaging and sensing require a sensitive measurement of bioelectromagnetic fields. In most cases, magnetic fields are measured with Magnetoencephalography (MEG) or Magnetic Resonance Imaging (MRI) using Superconducting Quantum Interference Devices (SQUIDs) [42, 43]. Electroencephalography (EEG) is an alternative to MEG, and uses electrodes to sense changes in bioelectric fields to monitor the same biological processes as MEG [44]. These techniques often suffer from poor resolution and excess noise, and in the case of SQUIDs require impractical cryogenic cooling. Therefore, other quantum techniques involving atomic magnetometry have been developed to increase resolution and practicality.

B.1 Classical

A wide range of techniques are used to do magnetic field sensing, and many of these techniques rely on classical electromagnetic effects. For example, in the case of Microelectromechanical Systems (MEMS) based magnetometers, motion induced by the Lorentz force can be electronically or optically detected to measure the magnetic field [45]. MEMS magnetometers are widely used due to their small size [46], however many such classical magnetometers suffer from poor sensitivity [47], and therefore cannot generally be used for biological applications. In fact, systems that are currently used for measuring biomagnetic fields such as MEG and MRI scanners rely on SQUIDs, which already exploit quantum effects in superconducting loops containing two Josephson Junctions [48].

The working principle of a SQUID device is as follows. If a current I is input into the loop, it splits equally in the two branches. If the loop is then exposed to a small magnetic field, a screening current I_s will be induced to oppose the magnetic field, and I_s will be in opposite directions in each branch of the loop, giving a current of $I/2 + I_s$ in one branch and $I/2 - I_s$ in the other branch. As soon as the applied magnetic flux exceeds half the magnetic flux quantum, $\phi_0/2$, it is energetically favourable to increase this flux to ϕ_0 since the flux in the superconducting loop is quantised by integer multiples of ϕ_0. Therefore, the screening current flows in the opposite direction, and this happens periodically, giving rise to an oscillatory current with a period of ϕ_0. The critical current, which is the current at which the junction starts to exhibit resistive behaviour, therefore also oscillates with an increasing applied magnetic field. This means that a change in applied magnetic field gives rise to a change in the output current of the junction, and therefore, by measuring the voltage leaving the junction, the external magnetic field can be measured [49]. EEG measurements are used to record the electrical activity in a subject's brain, and require a simpler apparatus than MEG and MRI [50]. In this procedure, a direct measurement of electric fields is performed by placing an array of electrodes on the subject's head, before amplifying and filtering the electrical output to monitor neural activity.

B.2 Quantum

B.2.1 Atomic Magnetometers

Many different techniques have since been shown to harness the quantum effects of photon-spin interactions to improve the precision and practicality of magnetic field measurements. The first of these techniques utilises an atomic magnetometer in which an ensemble of atomic spins is optically prepared and measured in the presence of a magnetic field [51–57]. The spins are polarised by optical pumping with a laser beam, and undergo Larmor precession due to the magnetic field. This precession leads to an oscillating component of magnetisation on the laser beam axis, leading to a periodic variation in the absorption properties of the vapour, and a corresponding change in the quadrature observables which can be measured to derive the magnetic field strength. This technique has been used to perform magnetic field sensing with quantum-noise limited uncertainty, as the noise that limits the measurement is due to the fundamental uncertainty associated with the projection of the spins into a state corresponding to the measurement, in addition to the quantum shot noise associated with the stochastic nature of the measurement of photons [58]. It is possible to create very compact and portable magnetometers using this technique, and figure B.1 shows a design for a microfabricated optical magnetometer which demonstrated very high sensitivities of $20\,\mathrm{fT\,Hz^{-1/2}}$ [52]. This sensitivity is high enough for biomagnetic field measurements, and comparable to record SQUID sensitivities of $3.6\,\mathrm{fT\,Hz^{-1/2}}$ [59].

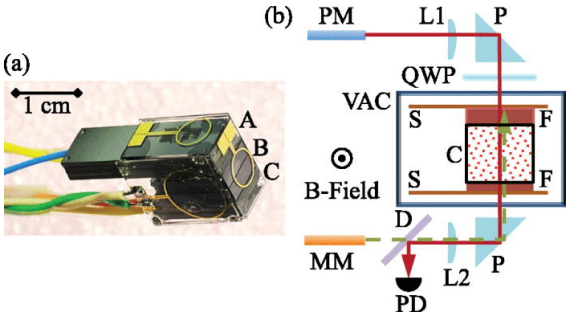


Figure B.1: (a) Photograph of a microfabricated optical magnetometer sensor. The size of the sensor head is approximately $0.36\,\mathrm{cm^2}$. The fibre for the probe beam is held in structure A, the atomic vapour cell in structure B, and the photodetector and heating light fibre in structure C. (b) Diagram of the magnetometer, showing the vapour cell illuminated by the probe beam (solid red line) and by the heating light (dashed green line). PM: Polarization maintaining optical fiber; MM: multi-mode optical fiber; L1, L2: lenses; P: reflecting prisms; QWP: quarter-wave plate; VAC: evacuated enclosure; S: polyimide web; F: optical filter; C: vapour cell; D: dichroic mirror; PD: photodiode. Image taken from [52].

B.2.2 Enhancement with Quantum Correlations

Despite this progress, further improvements in measurement precision have since been made to this setup by using Quantum Non-Demolition (QND) measurements and spin-squeezing [60–63]. The experimental setup for the QND magnetometer in [62] is shown in figure B.2. In these measurement schemes, a pump beam is used to spin-polarise the atomic vapour, meaning that a linearly polarised probe beam undergoes Faraday rotation when passing through the vapour. A QND measurement

of this polarisation rotation is used to determine both the magnetic field strength and project the ensemble into a spin-squeezed state, in which the sensitivity of subsequent measurements is decreased.

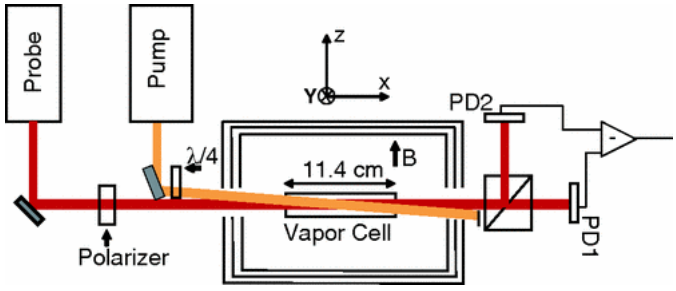


Figure B.2: Diagram of the experimental apparatus for a typical QND atomic magnetometer. A pump laser is used to spin polarise the atomic vapour, and a linearly polarised probe beam is directed along the length of the cell. Paramagnetic Faraday rotation induced by the atoms is measured with a balanced polarimeter, from which the magnetic field can be derived. Image taken from [62].

A related method has involved inducing Einstein-Podolsky-Rosen correlations in two isolated vapour cells with an optical QND measurement of the Faraday rotation through both cells. These correlations correspond to two-mode squeezing that acts to reduce the spin projection noise. A different approach was taken by [64], in which QND measurements of the Faraday rotation were implemented with a vapour cell enclosed by mirrors, creating a multipass cell and increasing the interaction volume and hence optical rotation. This experiment resulted in the most sensitive scalar magnetometry experiment to date, with a magnetic field sensitivity of $0.54\,\mathrm{fT\,Hz^{-1/2}}$. Other atomic magnetometry experiments have instead used squeezed light sources to probe the vapour of atomic spins [65, 66], and this has also enabled measurements surpassing the quantum noise limit. A promising approach could be to combine a squeezed light source with a QND measurement technique, such that the squeezing of incident light acts to improve the measurement sensitivity and the spin-squeezing of the atomic ensemble [67].

B.2.3 Nitrogen Vacancy Centres in Diamond

An alternative approach to exceed the standard quantum limit in magnetic sensing is to use Nitrogen Vacancy (NV) centres in diamond, which are defects consisting of two displaced carbon atoms in diamond, with one vacancy being filled by a nitrogen atom and the second left vacant [68]. The presence of unpaired electrons in the vacancy site gives rise to a quantum spin state that can be optically manipulated and measured, and has long decoherence times even at room temperature [69]. In the presence of a local magnetic field, the electron spin in the NV centre precesses, and this magnetic field may be measured with pulsed spin-manipulation schemes, in which this electron spin resonance can be optically detected [70–74]. One method of detecting the magnetic resonance of these NV spins is optically monitoring the NV centre by placing it on the end of a cantilever close to the magnetic field source and doing confocal microscopy. An alternative method involves embedding the NV centre on the tip of a tapered optical fibre in the presence of a local magnetic

field, and using this optical fibre for detection of the photoluminescence. Both of these techniques are illustrated in figure B.3.

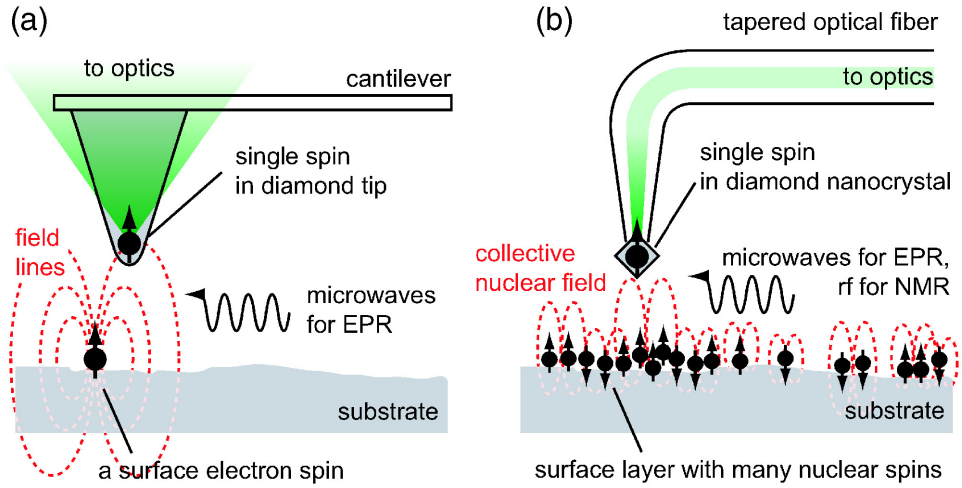


Figure B.3: Schematic of a diamond-based scanning spin microscope. Changes in the local magnetic fields will result in a shift of the electron spin resonance (EPR) frequency, and these magnetic fields can be measured by monitoring the corresponding change in photoluminescence of the probe spin. In (a), a single electron spin in an NV centre on the tip of an Atomic Force Microscope (AFM) cantilever is monitored using optically detected magnetic resonance with a confocal optical microscope. In (b), the shift in EPR frequency determines the change in magnetic coupling to an ensemble of spins, and the scanning probe also acts as an optical waveguide to detect the varying photoluminescence. Image taken from [71].

However, all the previous examples have involved magnetometry of the local magnetic field from a single electron spin. While this is a remarkable achievement, it is difficult to imagine how this technique may be used for measuring the magnetic field emitted by remote objects, such as a human heart or brain. Figure B.4 illustrates an example of how this may be achieved, by measuring the photoluminescence from a larger sample of diamond.

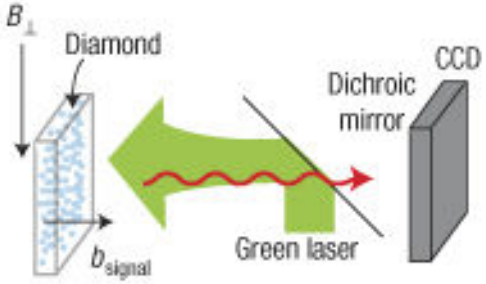


Figure B.4: This schematic illustrates a bulk dimaond magnetometer with a high density of NV centres for sensing fields created by remote objects. Here, a laser beam directed onto the sample induces spin-dependent photoluminescence, which can be detected using a Charge Coupled Device (CCD). Image taken from [73].

It can be shown that with an NV centre consisting of a single electron spin, the fluctuations in the detuning ω due to the Zeeman splitting induced by the target magnetic field are bounded by $|\delta\omega| \approx 1/\alpha\sqrt{M}T_{2e}^*$ [75], where α is a small constant and T_{2e}^* is the dephasing time of the electron spin.

Therefore, the electron dephasing limits the precision of the magnetic field measurement. A possible improvement to the setup due to this limitation has been proposed, which uses a hybrid system of an electron spin and a nuclear spin in an NV centre in diamond [75]. In this system, the electron provides a strong magnetic field coupling and so acquires a phase shift from the local magnetic field. The electron and nuclear spins are coupled via the hyperfine coupling, and it is therefore possible to transfer the information encoding the magnetic field strength from the electron to the nuclear spin. The nuclear spin is then used to store the phase information from this magnetic interaction, as the nuclear spin has a much longer coherence time. The bound on the precision with this hybrid system was shown to be $\sqrt{N}$ times smaller than the scheme involving one electron, where N is the number of times information is transferred from the electron spin to the nuclear spin before performing an optical measurement of the system. It is possible to perform several transfers of information between the electron and nuclear spin before the nuclear spin dephases, and hence this technique could enable the possibility of measuring magnetic fields with sensitivity far beyond that of previous magnetic sensors [76].

While this research in magnetometry with NV centres offers many ideas for substantially improving the achievable sensitivity, it should be noted that these techniques have not yet shown sensitivities much lower than $\sim 1\,\mathrm{fT\,Hz^{-1/2}}$ [77]. Therefore, atomic magnetometry is currently the only approach that has demonstrated quantum enhanced sensitivity beyond that achievable by SQUID techniques, although magnetic sensing using both NV centres and atomic magnetometers demonstrate promise in terms of portability.

B.3 Discussion

It is clear from this discussion that the field of quantum enhanced magnetic sensing is very broad, and many different approaches show promising results towards achieving enhanced precision magnetic field sensing with more portable devices that do not require cryogenic cooling. The primary application of these systems will likely be in medical diagnosis, such as quantum enhanced MRI/MEG scanning. The practicality and reduced cost of these devices could lead to a much wider distribution across hospitals and doctor's surgeries. Also, the possibility of home installation of such quantum enhanced medical tools in the future could significantly improve the rate of early diagnosis of many health conditions. However, at this early stage of technological development it is difficult to determine how cost effective such a large production of quantum enhanced medical scanners could be.

A far more specific application of quantum magnetic sensing is for a brain-computer interface for the control of wheelchairs for people suffering from paralysis. Previous designs for mind-controlled wheelchairs have all used EEG [78–80], as this is the only sensor capable of measuring the magnetic field of a person's brain which is portable and doesn't require cryogenic cooling. However, with the development of portable and non-invasive magnetic field sensors with quantum-enhanced precision, quantum magnetic sensors could be a very suitable application for this technology. This links to current research that is being undertaken into implants containing arrays of electrodes that could

be interfaced directly with the cerebral cortex in order to form a brain-computer interface [81, 82], mapping the activity of individual neurons. It is possible that the quantum magnetic sensing techniques discussed above could provide the necessary precision to achieve similar results non-invasively. However, it is also possible that the sensors would need to be brought into close proximity to the individual neurons to achieve the sensitivity required. If this is the case, then the approaches using an atomic vapour or optical readout of electron spins would not be applicable in a sensor which must be injected into the brain. Nonetheless, if the desired resolution could be reached with the methods discussed above, a brain-computer interface using quantum-enhanced magnetic sensing could find application in controlling prosthetics and allowing paralysis sufferers to move and communicate.

C Quantum Enhanced Cameras

Throughout the ages, man learned how to obtain and use light as he pleased. Starting from taming fire in the stone age, man developed multiple light sources, e.g. torches and candles, then progressed towards the practical electric light bulb by the works of Thomas Edison in 1879, until reaching the coherent light sources, like lasers, in 1960 with Theodore H. Maiman. Light sources prior to the laser, like the light bulb, emit thermal light, i.e. the atoms in such sources radiate independently, with no relationship between the phases for independent atoms. The laser represented a huge breakthrough for light sources as it emits a distinct type of light, called coherent light. A light source is said to be coherent when its atoms radiate with a constant phase difference and the same frequency. This allows much more powerful, concentrated and collimated light sources. These characteristics found great applicability in medical areas. Straightforward examples are cancer diagnosis [83], cancer treatment [84], melanoma treatment to scar revision, skin resurfacing, laser hair removal and tattoo removal [85].

Similar to creating light, mankind has a long history of detecting it. Already having our natural light detector, the eye, man later developed the camera and the photograph in 1826, which allowed us to store light information (not the light itself) in images. Since then, better and better cameras were developed. Now companies deliver professional cameras and mobile phones with better resolution and characteristics, e.g. anti-blur modes, various focal planes, and adjustable field of view.

Both light sources and light detectors can benefit from a variety of different quantum principles. We shall focus on two particular quantum principles, namely of photon entanglement and squeezed light, which already showed results in biological and medical areas, and which can have an impact on the camera and mobile phone industries by enhancing their resolution and sensitivity.

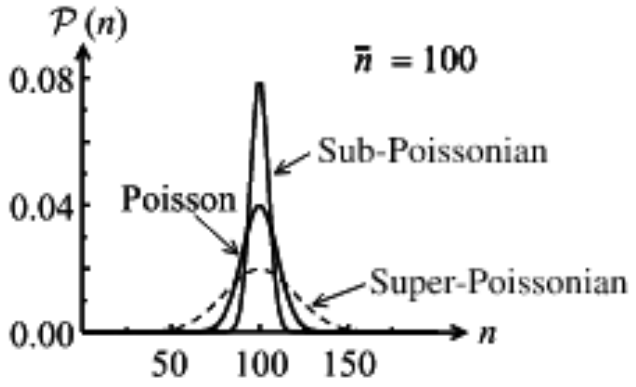
C.1 Classical

Before moving on to the quantum analogue, we shall briefly describe the classical version of both light sources and cameras.

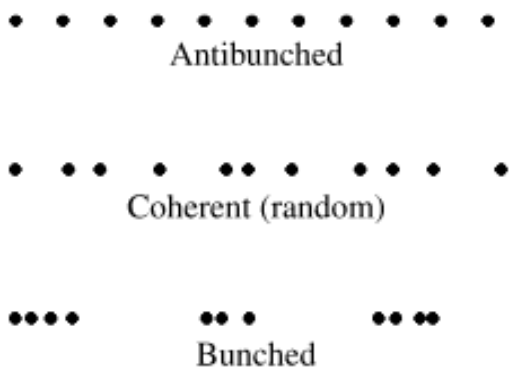
C.1.1 Light Sources

A light source can be characterised by the light it emits. As mentioned before, there are classical sources like the light bulb that emit thermal light, and classical light sources like the laser that emit coherent light. We classify these light sources using some of their properties. The first property we mention is photon statistics.

Light can be thought of being made up of photons. If we take different parts of the light wave, the number of photons in it will fluctuate per unit of time around a certain mean $\bar{n}$. This fluctuation is expressed by the standard deviation Δn. Light is classified depending how large $\bar{n}$ is compared to Δn. More specifically, there are three possibilities:



(a) Comparison of the photon statistics for light with a Poisson distribution, and those for sub-Poissonian and super-Poissonian light.



(b) Comparison of the photon streams for antibunched light, coherent light, and bunched light.

Figure C.1: Different features for classifying light. Image taken from [86].

- sub-Poissonian statistics: $\Delta n < \sqrt{\bar{n}}$,
- Poissonian statistics: $\Delta n = \sqrt{\bar{n}}$,
- super-Poissonian statistics: $\Delta n > \sqrt{\bar{n}}$.

Thermal light has super-Poissonian statistics and coherent light follows Poissonian statistics. The sub-Poissonian statistics is a characterisation of quantum light sources.

Another classification of light is by the degree of coherence $g^{(2)}$, which measures the correlation between pairs of fields, or, in other words, finds the statistical character of intensity fluctuations. It is defined as [86]

$$g^{(2)}(\mathbf{r}_1, t_1; \mathbf{r}_2, t_2) = \frac{\langle E^*(\mathbf{r}_1, t_1) E^*(\mathbf{r}_2, t_2) E(\mathbf{r}_1, t_1) E(\mathbf{r}_2, t_2) \rangle}{\langle |E(\mathbf{r}_1, t_1)|^2 \rangle \langle |E(\mathbf{r}_2, t_2)|^2 \rangle}.$$

Informally, the degree of coherence $g^{(2)}$ measures how bunched the photons are (see Figure C.1). Using $g^{(2)}$, we can divide light into:

- bunched light: $g^{(2)}(0) > 1$,
- coherent light: $g^{(2)}(0) = 1$,
- antibunched light: $g^{(2)}(0) < 1$.

The thermal light has $g^{(2)}(0) > 1$, so it is bunched, while lasers have $g^{(2)}(0) = 1$, so it is coherent. Antibunched light is a purely quantum optical phenomenon.

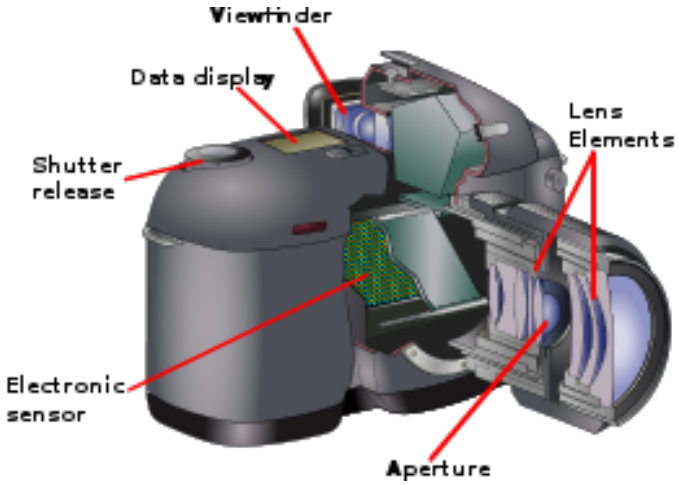


Figure C.2: Basic elements of a modern camera. Image taken from [87].

C.1.2 Cameras and the Diffraction Limit

As a brief description, a modern camera is an optical device which creates a single image of an object or scene and records it on an electronic sensor or photographic film. All cameras use the same basic design: light enters an enclosed box through a converging lens/convex lens and an image is recorded on a light-sensitive medium (see Figure C.2). A shutter mechanism controls the length of time that light can enter the camera. It is then important to note that cameras do not produce their own light, but instead capture the environment light. Since light emitted and reflected by everyday objects is chaotic, i.e. has super-Poissonian statistics, the performance of classical cameras will be bound by the limits of classical light. One of these limits is the diffraction limit.

Even though the resolution of an optical imaging system, such as the camera, can be limited by factors such as imperfections in the lenses or misalignment, there is a fundamental maximum to the resolution of any optical system which is due to diffraction, called the diffraction limit. The diffraction limit can specified by the Airy disk, which is a description of the best focused spot of light that a perfect lens with a circular aperture can make. The radius of the disk is given by

$$\xi_{classical} = 0.61\frac{\lambda L}{R}.$$

where λ is light wavelength, L is the distance between the object and the detector (or screen) and R is the lens radius.

C.2 Quantum

One characteristic that quantum technologies can improve for cameras is their resolution, i.e. the diffraction limit. This is achieved by coming up with novel light sources, e.g. sub-Poissonian and

antibunched light previously mentioned. We shall mention two kinds of quantum light that can impact the future of imaging and cameras.

C.2.1 Entangled Photons and Beyond the Diffraction Limit

Entanglement is one of the most striking features from quantum mechanics and has no classical counterpart. Quantum entanglement is a physical phenomenon that occurs when pairs or groups of particles are generated or interact in ways such that the quantum state of each particle cannot be described independently of the others. Mathematically, consider that a particle A is in the quantum state $|\psi\rangle_A$, while a particle B is in the quantum state $|\phi\rangle_B$. Thus we write that the quantum state of the whole system is $|\psi\rangle_A \otimes |\phi\rangle_B$. But it can be the case that the state of the whole system $|\Psi\rangle_{AB}$ cannot be written as a tensor product of two separate states, i.e. as $|\psi\rangle_A \otimes |\phi\rangle_B$. We then say that both particles are entangled. A basic example is $(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)/\sqrt{2}$.

It has been shown that entangled photons can enhance the spatial resolution of imaging beyond the classical diffraction limit [88,89]. Theoretically, it has been shown that $N+1$-photon entanglement improves the classical diffraction limit by a factor of N (but it decreases the visibility by N) [89]. More specifically, considering the Airy disk mentioned before, we can reduce its radius to

$$\xi_{quantum} = 0.61\frac{\lambda L}{RN}$$

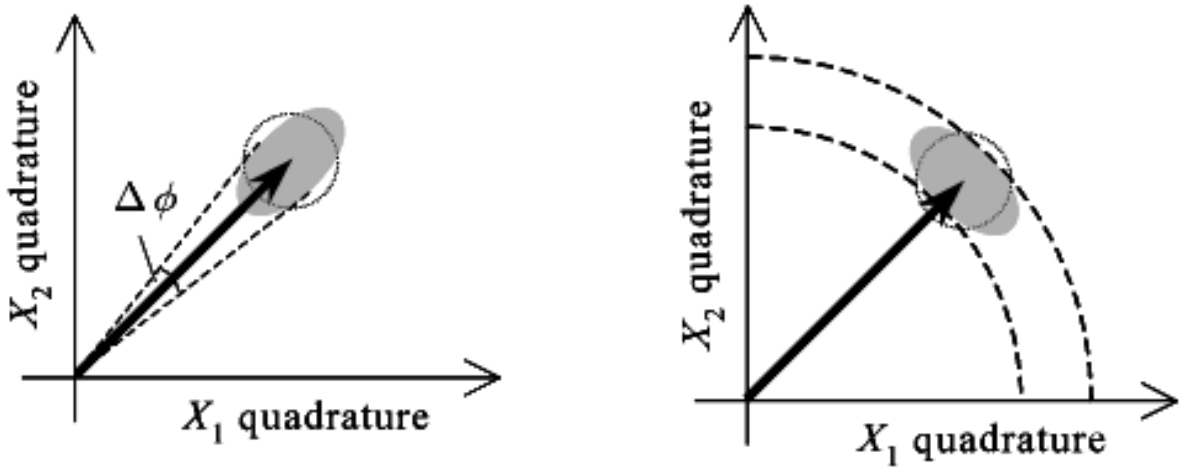
using $N+1$ entangled photons, which is N times smaller than the classical case and hence this presents a sub-Rayleigh resolution. The way this is done is by sending N degenerate photons to the object, keeping the non-degenerate photons and imaging lens in the lab, and use a resolving N-photon detector or a bucket detector (single-pixel detector that views the object). The image obtained is nonlocal and the quantum nature of the state leads to the sub-Rayleigh imaging resolution with high contrast. The straightforward advantage is a much better image quality compared to classical cameras.

C.2.2 Squeezed Light

Another physical principle which can be used to reach sub-Rayleigh resolution, much like the entangled light, is that of squeezed light. The quantum state of the light can be described via two special operators $\hat{X}_1$ and $\hat{X}_2$ (also written as $\hat{q}$ and $\hat{p}$) called quadratures. These quadratures have associated uncertainties given by the light state, which must obey an uncertainty principle like

$$\Delta\hat{X}_1 \Delta\hat{X}_2 \geq 1/4.$$

We say the light is squeezed along a given quadrature when the uncertainty of this quadrature is less than $1/2$. This can be represented schematically in the phasor diagram (diagram with $\hat{X}_1$ and $\hat{X}_2$ as axes) as an ellipse (see figure C.3). Two important squeezed states are the phase-squeezed light and amplitude-squeezed light, which have decreased uncertainty in the electromagnetic wave's phase



(a) Phase-squeezed light.

(b) Amplitude-squeezed light.

Figure C.3: Quadrature squeezed states. The dotted circle in each of the diagrams shows the quadrature uncertainty of the states with $\Delta X_1 = \Delta X_2 = 1/2$. Image taken from [86].

and amplitude, respectively. This means that the use of phase-squeezed light allows interferometric measurements with greater precision than that obtained with a classical light. Similarly, the use of amplitude-squeezed light gives smaller amplitude noise than that of a classical light.

C.3 Discussion

As mentioned before, the advantage of having a camera which uses non-classical light is a much better image quality compared to classical cameras. It is important to note that, different to classical cameras, which just capture external light, quantum cameras will need to produce these special quantum states of light inside them, shine the light onto objects and collect it. Either by mapping the environment light into entangled photons and detecting them, or creating and collecting squeezed light, all inside the cameras, which will require specialised detectors (N-photon detectors or bucket detectors), it can be possible to enhance the spatial resolution and improve the quality of the photograph.

On the one hand, one of the greatest challenges to overcome in order to achieve this technology is the entanglement itself. Entangling photons is extremely hard, especially if N is large. The current record for photon entanglement is 10 photons [90]. From this we can easily see how the quantum camera scales. As we entangle more photons, the better the enhancement, but the harder it is to achieve this enhancement. Moreover, these experiments for generating entanglement are based on bulk optics, which can easily take a whole room. An additional challenge will be to compress these experiments if it is supposed to be part of a camera. Also, in order to obtain information from the environment, it may mean entangling thermal light, but there has been some improvement in this direction over the past few years [91, 92]. All these facts lead us to believe that a quantum enhanced camera will probably take more than 30 years to be developed. One important milestone

will definitely be a process to easily generate entangled photons. Although there have been some experiments which achieved one-million-mode continuous-variable cluster states [93, 94], it is still necessary to ascertain if this kind of state is useful for imaging.

On the other hand, the problem of entanglement can be avoided if one uses squeezed light. The generation of squeezed light is much easier, since it can be achieved with bulk nonlinear optics using high intensities, and it was first generated 30 years ago [95], having then already found some applications, e.g. in medical areas and biology, interferometric measurements with gravitational waves [96], spectroscopic signals [97] and atomic clocks [98]. Regarding biology, it was already used to image a living cell [99] and to study proteins [100]. However, it does not present the same improvement over sensitivity as does the use of entangled photons.

D Quantum Dots for Biosensors and Chemical Sensors

Fluorescence is the effect whereby light is emitted by an object, in response to absorption of light by the object. In the quantum picture, the absorbed photon excites an electron to a higher energy state, which then relaxes back to the ground state, emitting its excess energy as a new photon. The emitted light is often at lower energy than the absorbed light, due to intermediate energy levels which allow relaxation in several steps. In molecules, closely spaced intermediate levels representing vibrational states occur and the shift in wavelength due to vibrational relaxation is known as Stokes' shift.

In biology, fluorescence microscopy is a popular technique for studying many kinds of processes involving cells, microorganisms and proteins. A solution containing fluorescent objects, or fluorophores, is added to the sample, and the fluorophores selectively attach to entities of interest. The sample is then irradiated with Ultraviolet (UV), and the visible light emitted by the fluorophores observed. The technique only differs from conventional microscopy by the addition of the fluorophore and the use of a UV source instead of a white-light bulb; in fact conventional microscopes can usually be converted for fluorescence imaging [101].

Fluorescence microscopy has matured to commercial devices, which are enabling much more rapid medical diagnosis than the traditional method of culturing the sample [101], i.e. waiting several hours for the pathogens to populate a nutrient medium for detection by eye. There is now some effort to adapt the technique for automatic detection in portable devices, known as biosensors. One example is a detection scheme for gliadin (a class of proteins found in gluten) for use by people with Celiac disease. The fluorophore is based on two components: a sensor molecule which absorbs some ambient light, and a transducer which receives energy from the sensor molecule via Fluorescence Resonance Energy Transfer (FRET), and emits light [102]. The absorption of the sensor molecule changes significantly upon binding to gliadin, resulting in a detectable change in fluorescent light from the transducer.

D.1 Classical

Before 1998, there were two types of fluorophore: dyes and proteins. The dyes are fluorescent chemical compounds which bond to organic chemicals, for example the organic compound fluorescein [101]. Fluorescent proteins go a step further: by adding a fluorescent protein sequence to the target-protein sequence in the organism's DNA, we can make the organism produce fluorescent protein attached to the target-protein. This allows study of the target-protein production rate, by observing new fluorescent proteins appear. These have enabled many landmark studies in biology, for example the 'Brainbow' [103], and the fluorescence technique has been recognised by two Nobel Prizes in Chemistry: for the development of fluorescent protein in 2008 and for super-resolved fluorescence microscopy in 2014. However, both fluorophore types share a number of problems. The main problem is photobleaching, the loss of ability to emit light in response to the UV. This limits observation time to a few minutes [104].

D.2 Quantum

In 1998, a new type of fluorophore was demonstrated - the QD [105, 106]. A quantum dot is a nanoscale particle of semiconductor material. This size is comparable to the extent of the electron wavefunction, causing quantum confinement. Quantised energy levels occur as a result, in contrast to the continuous conduction and valence bands found in bulk semiconductors. The semiconductor bandgap can be tuned by changing the size of the dot, to have an energy comparable to a visible light photon, illustrated in figure D.1. Fluorescent light is produced when an electron in the dot relaxes back to a valence state, after having been promoted to a conduction state by the UV.

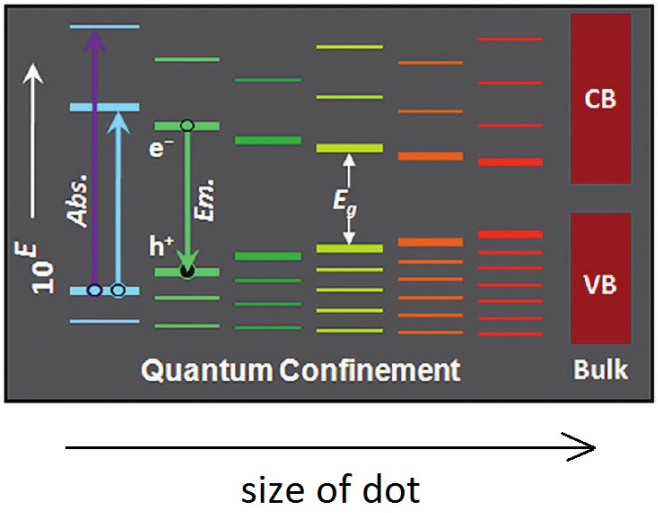


Figure D.1: Diagram illustrating the correlation between the diameter of the quantum dot and the size of the semiconductor bandgap. Colours indicate the larger dots produce light towards the red end of the spectrum as the electron transition across the bandgap is smaller. The purple arrow illustrates excitation across the bandgap by the UV source. Image taken from [107].

Quantum dots can be used in the same way as the previous fluorophores, after coating with some type of molecule, or *functionalising*. An entity of interest is targeted through the choice of molecules used to coat the QD, which determine what it will repel, attract or bond to.

D.3 Discussion

Quantum dots have proved much more resistant to photobleaching, and are brighter than the alternatives, giving higher quality images [107, 108]. Resistance to photobleaching has enabled the study of slower biological processes using QDs, such as the transport of large molecules though the barrier between nucleus and cytoplasm in human cells [109].

There are concerns about toxicity as the most popular material for the semiconductor contains the heavy metal cadmium, which is released when the dot breaks down. The most widely studied QD, simply due to ease of fabrication by the hot-injection method, is the CdSe dot with a ZnS shell [107].

Toxicity is mainly a problem for *in vivo* diagnostics, but leaves many useful applications for testing of samples *in vitro*. There is also promising work using carbon QDs, which were successfully used to image zebrafish embryos and larvae, and shown to be essentially non-toxic for low concentrations $\sim 0.5\,\mathrm{mg\,mL^{-1}}$, whereas the low-toxicity competitor maghemite@SiO_2 QDs caused severe deformities at $0.2\,\mathrm{mg\,mL^{-1}}$ [110]. Carbon QDs have been successfully functionalised, by coating with branched polyethylenimine, and used to detect Cu^{2+} ions [111, 112]. The Cu^{2+} ions reduced the fluorescence of the dots when attached to them (referred to as quenching), allowing measurement of the Cu^{2+} concentration [112], similar to the mechanism described above for the gliadin biosensor.

Using the same principle of fluorescence quenching, a system for detection and differentiation of explosives using QDs was tested [113]. As illustrated in figure D.2, three different colours of QDs were used, each type designed to attach to a different explosive chemical. The fluorescence spectrum was analysed to detect reduced intensity of one of the colours, indicating the presence of the corresponding explosive. The limit in sensitivity was estimated to be parts-per-billion. QDs are ideal for such multichannel sensing schemes due to their variety of colours and sharp emission peaks.

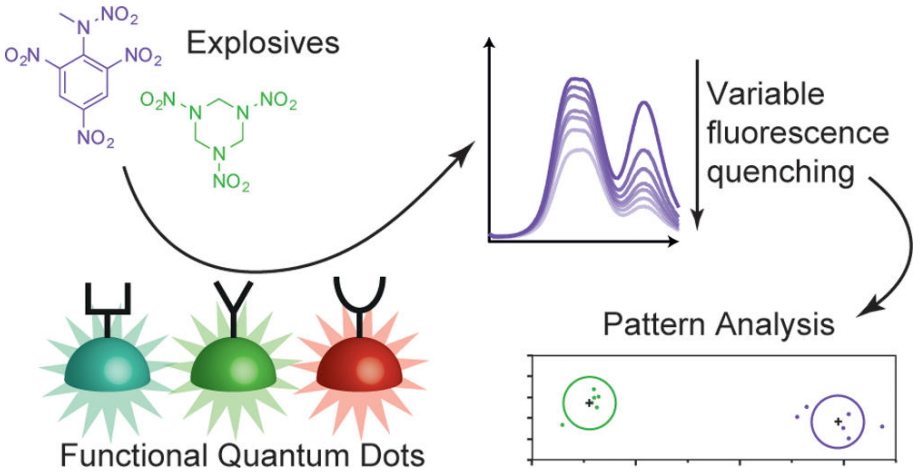


Figure D.2: Illustration of the quantum dot explosives detection scheme from [113].

QDs have been successfully used with several super-resolution imaging techniques such as Stimulated Emission Depletion (STED) microscopy and STochastic Optical Reconstruction Microscopy (STORM), enabling nanoscale resolution of single molecules' distribution. A resolution of 54 nm was achieved using QDs with STED, compared to the 230 nm resolution achieved by confocal microscopy [114]. However STED requires high-intensity laser pulses which can damage samples [115]. STORM builds up an image sequentially, by activating a fraction of the fluorophores such that they are sufficiently spread out to be resolved, then deactivating them and repeating for a different subset. The position of a single fluorophore can be determined to almost arbitrary precision after sufficient photons are detected, by averaging the positions given by each photon [115]. A resolution of 24 nm was reported with this technique using QDs [116]; the comparison with the confocal image is shown in figure D.3. Similar techniques exploit a unique property of QDs called blinking, when the fluorescence turns on and off intermittently. Observing blinking for a period of time allows individual QDs to be resolved, provided that there are not too many dots in a cluster, and the

off-time is not much shorter than the on-time. Two examples are Super-resolution Optical Fluctuation Imaging (SOFI) [117] and Quantum Dot Blinking with 3D Imaging (QDB3) [118], which can reportedly build up images faster than STORM.

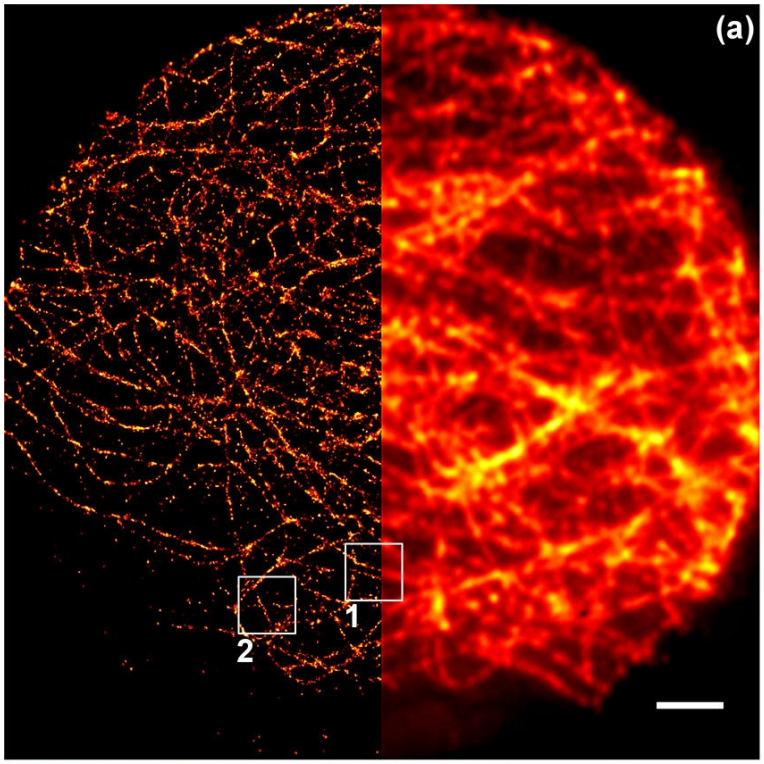


Figure D.3: Comparison of confocal microscopy (right) with super-resolution technique STORM (left), using 565 nm quantum dot fluorophores to label microtubules in HepG2 cells. Scale bar is 2μm Image taken from [116].

Properties other than fluorescence of QDs can be used to obtain additional information. An alternative proposition exploits 'photoinduced charge carrier transfer' [119], which means light is used to excite electrons in the dots such that an electron has enough energy to tunnel out of a quantum dot. This effect can be used to infer the concentration of oxidant molecules (electron acceptors) in a solution as follows. The electrodes are coated in QDs to which electrons can tunnel into the valence band. Electrons in the conduction band can tunnel to molecules in the solution, therefore under constant illumination, the photocurrent increases with acceptor concentration. The concentration of electron donors ('reducing' molecules) can be measured by the same technique, but with opposite current flow. The molecules can transfer electrons to the dots' valence band, which are excited to the conduction band and then able to tunnel to the electrode. The electron energy potentials of the molecules and electrodes need to be inside the dot bandgap for this to work properly; this implies selective discrimination of molecules in the solution. The technique has been used to detect simple molecules like oxygen [120] up to detection of the mismatch of DNA strands (although in this experiment QDs could detach from the electrodes and current was dependent on the number of attached dots) [121].

E Optical Port and Router

Every house with an internet connection has a router that connects the house to the backbone via other connections, allowing internet traffic to be routed through the network from any point to any other point on the network. This router also allows for connecting one object in the house to any other using Wi-Fi or Ethernet cables. As routers and switches are the methods currently used to connect somewhere to the internet, they are also used to perform secure data transfer. However, current classical security relies on computationally hard problems, such as RSA encryption [122], Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) [123,124], which could eventually be overcome if a large enough quantum computer could be made. As such, the method of encryption may need to change at some point. One way of ensuring security is to use QKD. Quantum technology also allows for improved methods of data transfer, such as using increased speeds or quantum teleportation.

E.1 Classical

Currently, a router works by sending data in the form of a classical electric signal through a twisted pair cable to the next highest gateway, which in turn decides where to send the signal next so that the data reaches its desired location in the fastest time with the least loss possible as in figure E.1. As the cables from a home router are not fibre, the signal is often converted from an electrical signal along a cable to an optical signal along an optical fibre allowing for both faster and more data transfer, as described by the Institute of Electrical and Electronics Engineers (IEEE) 802.3: Ethernet standard [124], as part of the IEEE 802 standard for Local and Metropolitan Area Networks, which also gives the standards for wireless networks of various purposes and sizes.

Anything that accesses a network will then have either a wired port (used with an ethernet cable) or a wireless port. It can then use the same principle as above, where it sends data using either ethernet or wireless to the router, which decides whether to forward this to the next level in the network as above, or whether to send it to another device within the same Local Area Network (LAN).

Aside from improving the security of these systems, there is a continual, gradual improvement in the amount of data that can be transmitted, using various different methods such as Orthogonal Frequency Division Multiplexing (OFDM) [126–128], where multiple orthogonal frequencies are sent at the same time to increase the amount of data sent; cable shielding to reduce noise; and using multiple pairs, as described in the International Organization for Standardization/International Electrotechnical Commission Final Draft International Standard (ISO/IEC FDIS 11801 standard) [129].

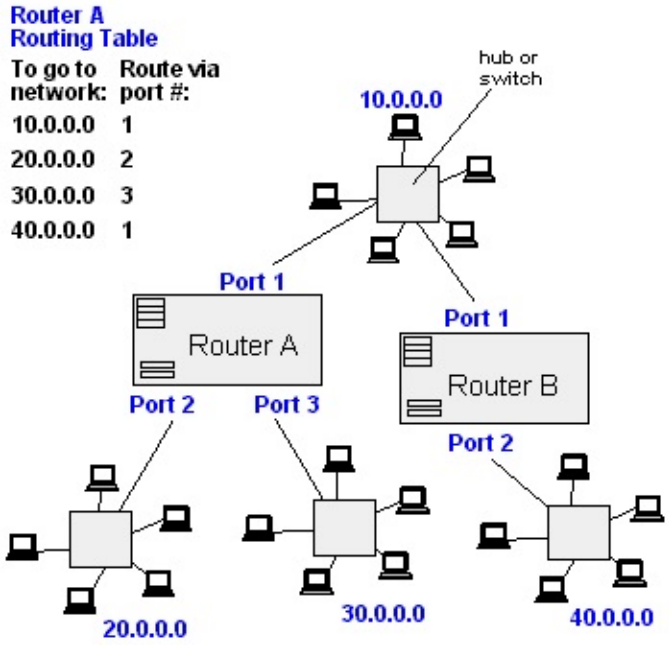


Figure E.1: Route forwarding protocol. Packets containing the final IP address are sent through a port to a router, which decides which port to transmit the packet along based on the IP address in the header of the packet. This process repeats until the data reaches its final destination. Image taken from [125].

E.2 Quantum

The ability to send a quantum signal in the form of a stream of single photons or an attenuated coherent state from any place to any other place that it is connected to would have potential uses, such as QKD, superdense coding enabling twice the rate of data transfer if single photon states could be generated in the future at a reasonable cost [30, 130, 131], quantum state teleportation, where the state is sent from transmitter to receiver [132], authentication (as, for example, in Article F) and Blind Quantum Computation (BQC), where the router connects to a quantum processor, explained in Article G to perform a computation where the computer performing the computation is unaware of the computation being performed [133]. However, in order to do any of these, it would need to be possible to send some form of quantum signal through a network such as the internet. It is possible to send quantum signals in free space over large distances, such as over a few km to a moving receiver [134], over a few hundred km to a fixed receiver [135] or even to satellites [136, 137].

E.3 Discussion

E.3.1 Quantum Routers

While quantum signals (in the form of single photons, or alternatively, a strongly attenuated coherent state) can be sent through an optical fibre, there are several issues with sending or receiving such a signal from a house. The first issue is that the connection from a house to a higher level in the network is usually copper, not fibre. This is easily fixed (if at considerable expense) by replacing all the copper cables to optical fibres. This can also be fixed by performing free space quantum communication to the nearest gateway that uses fibre, such as in [138], or using satellites, such as in [136, 137, 139].

However, the other issues are more problematic. The first is that loss in fibre at $0.1 - 0.2\,\mathrm{dB\,km^{-1}}$ is too great to send single photons over large distances. As amplifiers don't work for single photons, the network needs to become a quantum network using either repeaters [140,141], where one photon from each of two pairs of entangles photons is put through a beamsplitter and measured, as in figure E.2; trusted nodes, where the signal is measured at each node, then a new signal containing the data of the original signal is sent to the next node. This could be implemented, albeit not very well, with current technology at a monumental expense, although this cost should decrease considerably in the future. These nodes could be combined with the above network route forwarding protocol in figure E.1 to share entangled states between arbitrary nodes in a network and perform quantum communication protocols between these nodes. The maximum distance achievable using repeaters would be an improvement over not having any repeaters as the entanglement rate decreases exponentially with the square root of the distance using repeaters, compared with decreasing exponentially with distance when no repeaters are used.

This cost is due to the biggest problem of generating and measuring single photons. Current technology can create states where the average number of photons in a pulse is < 1 by strongly attenuating a laser, although at the cost of £100,000 per box [142, 143]. This is sufficient for QKD, which allows for secure data transmission between A and B. A cheaper method than this would be to use Light Emitting Diodes (LEDs), as in Article F.

E.3.2 Quantum Key Distribution

The first QKD protocols, such as BB84, were a series of photons that are polarisation encoded by a random number generator and transmitted to a device that measures these single photons. The bases used and measured are then compared between sender and receiver. A percentage of the polarisations where the correct bases were used are then compared between the sender and receiver and receiving a percentage of incorrect polarisations above a threshold value after the protocol indicates an eavesdropper as shown in figure E.3 [144]. This is more secure than just using a password or any of the above classical security protocols and has been proven to be secure both theoretically and experimentally [145, 146]. Many current commercially available methods of QKD

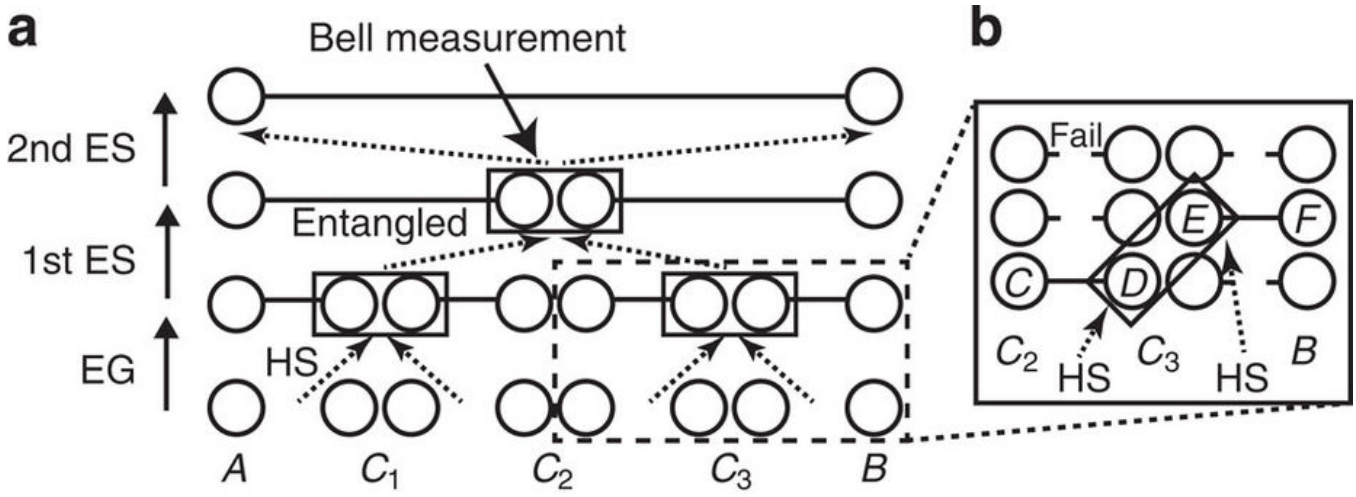


Figure E.2: a) basic repeater protocol involving creating entangled pairs of signal and idler photons (Entanglement Generation, EG) between neighbouring nodes and recursively calling the Entanglement Swapping (ES) operation where the photons of a node are heralded (heralding signal, HS) in order to probabilistically entangle nodes that are further apart. b) the same procedure where each node has multiple memories to help increase the success probability using multiple memories so that, when an EG or ES operation fails, there are other successfully entangled bits that can be used for further ES operations. Image taken from [141].

involve protocols such as Coherent One Way (COW) [143, 147] and SARG [142, 148], which work using attenuated lasers with an average number of photons, $\mu < 1$ and encoding the qubits using orthogonal bases.

Current rates for QKD are 10 Gbps (which would be the same as using these quantum states for non-secure data transmission using forward error correction, and more than an order of magnitude greater than currently possible with classical systems). Over 50 km, this reduces to 1 Mbps for secure transmission. Secure transmission is possible up to > 300 km, through fibre, > 100 km through free space, or > 1000 km using satellites. However, these speeds can be further increased using methods such as OFDM [149] by an amount depending on the number of channels used, possibly by at least another order of magnitude.

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

Figure E.3: Basic Idea of the BB84 Quantum Key Distribution protocol: Alice sends polarisation encoded photons using randomly selected bases from horizontal/vertical and diagonal/antidiagonal. Bob then measures the received photons using the same set of bases. These bases are then compared, along with a small sample of the received bits to validate the key exchange. Image taken from [144].

F Handheld Authenticator

With the advent of credit and debit cards, cash transactions are less and less frequent than they once were, with most cash withdrawals from an Automated Teller Machine (ATM). As a result of this change in how money is dealt with, a secure way of banking, withdrawing money and non-cash transactions is needed. As classical methods of doing these are often not secure, better methods need to be used.

F.1 Classical

There are a few different ways of authenticating someone's identity for monetary transactions and using an ATM. Currently, Electronic Funds Transfer at Point of Sale (EFTPOS) is frequently used (with the Europay, Mastercard and Visa (EMV) standards for chip cards and contactless cards [150]). Using a Chip Authentication Program/Dynamic Passcode Authentication (CAP/DPA) currently consists of inserting a credit/debit card into the CAP/DPA and inputting a Personal Identification Number (PIN). The machine then creates a pseudo-random number which is input as part of a login to online banking. An alternative to this is a system such as an indexed Transaction Authentication Number (iTAN), where the bank generates a list of indexed pseudo-random numbers. The user is told the index of the number to input when logging in, with each number being used once.

However, there are security flaws in EMV, CAP/DPA and one-time passwords/iTANs, many of which involve either tampering with the device or a man in the middle attack [151, 152]. In any form of classical communication, there is always the potential for a man in the middle attack to occur and these attacks are frequently avoided using more stringent communication protocols or more complicated technology. However, this in turn can just cause more complex attacks [153], with the potential to cause a continual battle between fraud and banks.

One way to help improve security would be to use a QRNG [154], such as in appendix H, which would potentially improve the security as security methods such as RSA, secure ID and iTANs all currently involve pseudo-random number generation, which, while usually practically secure with current technology levels, is not theoretically secure [155] and so, may be broken in the future.

As CAP/DPA machines are designed to be given to every customer, they are required to be cheap and so, also have potential security flaws [156] such as a man-in-the-middle attack, which has the potential to read these numbers and use them, pretending to be the consumer.

F.2 Quantum

To get around this potential flaw, the ideas of QKD, explained in appendix E, are adapted as explained below.

F.3 Discussion

F.3.1 Short Term

The bank would create random numbers (ideally using a QRNG or some other random process) that are then stored in a memory. Each bit of this random number is then used to create a single photon in either the horizontal/vertical or diagonal/antidiagonal basis. In the future, assuming a reasonably priced, reasonably fast, true, deterministic single photon generator exists, this would be used. Currently, as this doesn't exist, four LEDs, with each LED emitting one of horizontal, vertical, diagonal and antidiagonal light, are multiplexed and attenuated to the single photon level. This is sent through a diffraction grating for alignment as in figure F.1, then into a receiver and measured [157] as shown in figure F.2. This technology already exists and is shown in figure F.3. Currently, the transmitter is the size of a 2.5 cm thick credit card and could potentially be sold for approximately £10 each to a bank, which would buy one for every customer. Each bank branch would also have a receiver (a unit about the size of a standard PC, costing an estimated £100, 000). At the moment, functionality is limited to the transmitter having to be plugged directly into the receiver, which is of limited use in secure electronic banking due to the cost of the receiver making it infeasible for every bank customer to own one, as well as the security relying on the single photons being sent between the user and their bank, although in the future, a quantum port, such as in appendix E, could potentially be used to send the single photons through a fibre through a network to the bank.

Figure F.1: Four LEDs, attenuated to the single photon level, are placed behind polarisation gratings and angled to enter a diffraction grating at the same point, with the diffraction grating used to align the LED signals. Image taken from [157].

F.3.2 Long term

In the future, as well as using single photon generators, alignment would be done using free space optical tracking and alignment, such as a more condensed version of [158] and the same principle could be used to perform authentication over free space, even over large distances of several km, making usage easier without compromising security, although at a slightly reduced rate due to loss.

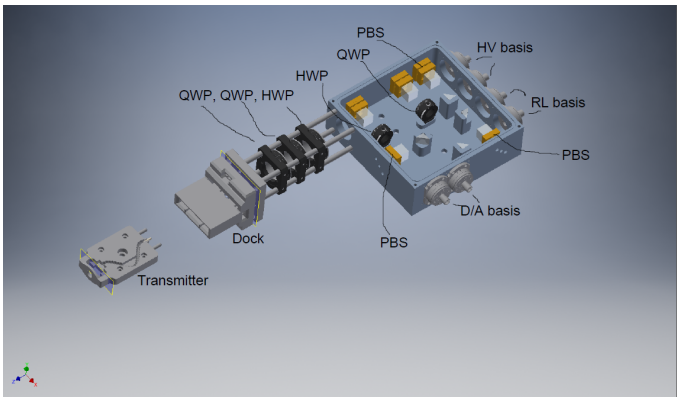


Figure F.2: Schematic of the receiving device used to perform handheld QKD. Image provided by Dr David Lowndes.

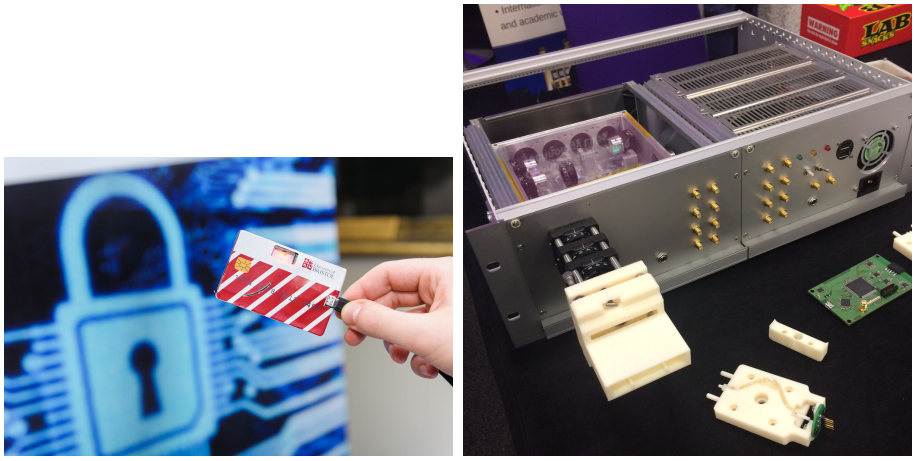


Figure F.3: Photographs of the transmitting (left) and receiving (right) devices used to perform handheld QKD. Image provided by Dr David Lowndes.

F.3.3 Other potential uses

This technology would also have other potential uses, such as remotely accessing another computer securely, or any other system where passwords are used, with the transmitter acting as a physical key that generates a unique electronic key each time.

As this is a physical object, it could also be used as a form of electronic lock, although until the cost of the receiver reduces, this is too expensive to be implemented on a large scale. This gives extra security due to the 'key', only able to be copied by the receiver that knows the bases of the measurement (which can be decided by another random number).

G Quantum Processor

Modern computing has changed the world over the last few decades. Since the invention of the transistor in 1947, the impact of computing has been felt in almost every section of society. Inside a modern PC there are several units capable of data processing. The most important of these are the Central Processing Unit (CPU) and the Graphics Processing Unit (GPU). While both these devices work on using the same (classical) physical principles, they are designed to be good at very different things. This specialisation is what allows a modern PC to perform the huge variety of work that it does. It is not too difficult to imagine some kind of Quantum Processing Unit (QPU)) that could sit alongside the CPU and GPU, specialising in tasks that these other two units cannot do efficiently (or even at all).

Of course, this hypothetical QPU will not operate using the same classical physics employed by the CPU and GPU. It will rely on the quantum mechanical principles of superposition and entanglement to perform calculations that are practically infeasible on a classical device. The ideal QPU would be a universal quantum computer, with the ability to take classical data from other parts of the computer and return classical output in a format that is useful to the rest of the machine. However, it is plausible that more specific devices could be used as a QPU for specific jobs. For instance, the work of M Amin et. al. [159] on using the D-Wave machine as a quantum Boltzmann machine could lead to a QPU specialised for certain machine learning applications.

G.1 Classical

A modern classical computer divides the work it does between the two primary processing units - the CPU and the GPU. The building block of both these devices, and in fact of almost all the electronics inside a PC, is the transistor. A transistor is a small (Intel has recently announced the creation of a 5 nm transistor [160]) device which is capable of behaving as both a switch and an amplifier. By arranging transistors together one can build logic gates, and from these gates a computer chip.

The CPU (with all it's associated cache, memory, etc) is the closest a PC has to a brain. It is capable of performing any logical or mathematical operation a computer can do, whether through native physical gates or through combinations of such gates. They are used to perform complex series of operations on relatively small amounts of data at a time, and manage the allocation of the computer's resources.

A GPU can be either a separate chip (a dedicated GPU) with its own dedicated memory or an integrated chip which shares memory with the CPU. The ideas behind each implementation are the same however. The main purpose of a GPU is rapid manipulation of memory with the aim of drawing images to the screen. This is accomplished by reducing the number of operations the circuitry can perform, but providing many parallel sets of such circuitry. This reduction in individual circuit complexity means that a GPU cannot quickly perform the variety of operations that are possible on

the CPU (although all are possible in principle, they will just be slow in comparison). What then is the advantage of a GPU? It comes in the massive amount of parallelism present in the design. A GPU is optimised to perform many simple operations on large amounts of data at once. Of course, this is only useful when the calculations to be performed are independent of each other but this happens fairly often in computing and hence GPUs form an essential part of a modern PC.

G.2 Quantum

Quantum computing is an area of intense research at the moment. The essential promise is familiar - a quantum computer will be able to solve problems that are practically infeasible for a classical machine, this speedup is provided by the machine taking advantage of superposition and entanglement. While a full description of the mechanics behind such a machine would take far more space than available here (see [30] for a complete description), here is a short (non-rigorous) summary of how a gate model quantum computation works. The exact details of how to perform these steps will vary based on the platform used to build the computer.

First we prepare a specific input state of n qubits, typically the equal superposition state.

$$|\Psi\rangle = \frac{1}{2^n}\left(|000...0\rangle + |000...1\rangle + ... + |111...1\rangle\right). \tag{1}$$

Use single and double qubit gates to manipulate the amplitudes of certain states - increase the amplitude of states corresponding to the correct answer and decrease that of incorrect answers.

$$|\Psi\rangle = \alpha_1 |000...0\rangle + ... + \alpha_c |\text{answer state}\rangle + ... + \alpha_n |111...1\rangle. \tag{2}$$

Here $\alpha_c >> \alpha_i \forall i \neq c$.

We then measure the state, obtaining a specific outcome (of some physical quantity) λ_i with probability $|\alpha_i|^2$. In the previous step we maximised α_c so that we obtain the result λ_c (the correct answer) with high probability.

The ideas presented here describe the behaviour of a gate model quantum computer. Other models of quantum computation exist, namely cluster state (also called measurement based) and quantum annealing. The cluster state paradigm performs computation by first building up a large state of many entangled qubits (the 'cluster' state), and then using measurements to selectively destroy certain links in the cluster [161]. This model has been shown to have the same computing power as the gate model [162]. Quantum annealing however is not a universal quantum computing paradigm. It aims to use quantum fluctuations to find the minimum of a function [163]. This has been implemented in superconducting circuits in a commercial system [164]. At the time of writing, no problem has been found that can be solved by this system faster or more efficiently, but work is ongoing [165]. Regardless if this specific model proves to be useful, the idea of a device using quantum mechanics to solve a certain type of problem without being a universal quantum computer is a viable way that QPUs could be implemented.

How exactly the initial state needs to be manipulated depends on the algorithm being run. The most well known algorithm is Peter Shor's - used to factorise integers exponentially faster than the best known classical algorithm [166]. However, more and more algorithms are being developed, a good summary of such algorithms can be found in ref [167].

In addition to algorithms, research on quantum computation looks at how we might practically build a quantum processor. Currently the leading platforms for a universal quantum computer appear to be superconducting qubits (worked on primarily at Google/University College, Santa Barbara), trapped ion qubits (worked on in the Networked Quantum Information Technologies (NQIT) Hub in the UK and Innsbruck in Austria) and photonic qubits (worked on in Bristol in the UK and Waterloo in Canada). It should be noted that each of these is worked on in multiple places besides those mentioned here. Each platform offers distinct advantages and disadvantages, and it is currently unclear which will prevail - or indeed if all platforms (including those not discussed here) will work together in yet more specialised roles.

G.3 Discussion

In thinking about a QPU, we can think about the properties it should have in order to be useful as a coprocessor in a modern PC. It must be able to interface with the devices, this can be done either electrically or optically with little change needed in the classical machine. It must be able to operate in the environment of a classical computer without significant extra hardware being needed. Finally, and most importantly, it must be sufficiently scalable to solve problems the classical hardware cannot.

Superconducting systems are the primary focus of industry backed research. The Martinis group at Google/University of California, Santa Barbara (UCSB) are currently aiming to demonstrate quantum supremacy in the near future [168]. Following from that, they have published work describing the commercial aspects of their work that they hope to realise in the next five years [169]. These goals are focused around problems that are more specialised than those solvable by a universal quantum computer - quantum chemistry simulations, quantum assisted optimisation and quantum sampling. In this way, they fit nicely into the model of a QPU being discussed here - solving specific problems that the classical hardware cannot. However, the low temperatures required for superconductivity may prevent the integration of these qubits into classical hardware, unless the cost of dilution refrigerators drops substantially. However, electrical connection between superconductors and standard electronics is possible [170].

Trapped ion qubits offer a key advantage over other systems, they have relatively long coherence times (both T_1 and T_2) available without as much engineering required. This is due to the nature of a trapped ion - there is simply very little else in the trap to interact with. The main focus of the UK NQIT hub is on trapped ion qubits arranged in small 'nodes' connected by optical fibre [171], though there are also proposals for large arrays of trapped ions controlled by microwaves and electic fields [172]. Both of these proposals aim to deal with the scalability issue that currently affects all platforms. In terms of acting as a QPU, ion traps also suffer from the need for cryogenic

temperatures which limits how easy integration with classical machines may be. However, ions interact very naturally with optical systems, which themselves are already integrated with classical machines in fibre optic internet connections.

Linear optics is the only one of the three platforms discussed here to not require cryogenic temperatures to operate in principle. Currently the best single photon detectors require superconducting electronics and hence a cryostat, but the process of computation can all be performed at room temperature. This presents a significant advantage as it makes the surrounding apparatus much less costly and easier to use. However, photonics use photons (as the name suggests) to form the qubit. As a general rule photons do not interact easily and therefore 2-photon gates in this model operate with low probability [173]. This has prompted a switch away from the gate model of computation implemented by other platforms towards a cluster state model [174]. The cluster state model uses measurements to break up large states of multiple entangled photons, to produce the same results as the model outlined above [161]. In terms of integration, photonics has significant advantages: it works at room temperature, modern implementations are based in silicon which means they may be able to be built onto the same chips as the main components of a PC, and optical/electronic interfaces are well understood.

Whether or not the QPU becomes a useful tool in personal computing depends on two things: the development of a platform that is easily integrable with classical machines (photonic systems seem to be the best candidate, but there is significant research needed before such a device is built), and the advent of a problem for a QPU to solve. This second requirement may currently present the bigger long term challenge. Whilst algorithms like Shor's and Grover's provide speedups for useful mathematical problems, they are not tasks that are often done in the home. Work is ongoing to find problems that may be of use in smaller scale machines. Examples include work on quantum Boltzmann machines for machine learning [159], quantum chemistry simulations [175] and quantum/classical hybrid systems for physical simulation [176]. Whilst each of these is also not a problem commonly solved in the home, they are also only the first steps in this research field - finding uses for non-universal quantum computers.

The inherent practical difficulties associated with the current generation of quantum devices may mean that they never appear in the home. However, a scenario involving sending requests to a quantum cloud service may be much more practical. BQC allows a classical client to send a request to a quantum server, which carries out the request while knowing nothing about what it is doing [133]. From a home user perspective, this is ideal: it allows access to a computational resource they wouldn't otherwise have, without the associated costs and difficulties of setting up a cryogenic environment in their own home. Most important to this protocol is the blind nature of it. This means that a user can send a request and get back an answer without the server that is carrying out the request knowing what it is doing. This is accomplished using entangled states, such that the server only ever sees a partial state which appears to be maximally mixed due to its lack of information about the global state. Combined with QKD, BQC allows a user to send a request to a server, secure in the knowledge that neither the computation nor the answer can be known by anyone else. This has obvious implications in privacy and computer security, especially given that a universal quantum computer already has the capactiy to break most modern cryptography.

It does not seem to be the case that the QPU will soon appear in home PCs. The lack of obvious problems requiring it, combined with the immense practical obstacles mean that, if it does appear, it is unlikely to be in the near future. Routes such as BQC may provide a halfway house of sorts, allowing access to quantum resources when necessary while not requiring every home to have access to a cryostat.

H Random Number Generation

Randomness is an exciting concept. Since the period of Epicurus and Democritus there has been a discussion about whether nature is deterministic or not [177,178]. Within the framework of classical physics there is no real randomness. The probabilities appearing in classical physics reflects only our lack of knowledge about aspects of a physical system. This kind of randomness is the so-called "subjective', 'epistemic' or 'apparent' randomness [177]. Imagine for example the experiment of flipping a coin. If we knew exactly the initial conditions of the motion of the coin and of the air molecules, then, according to the laws of classical mechanics, we would predict the outcome with absolute certainty [179, 180].

Quantum theory introduced a new kind of randomness. In quantum theory even in the case where we know exactly the preparation of the state of a physical system, the best predictions we can make about it are still probabilistic! [179] This is the so-called 'fundamental', 'ontic', 'intrinsic' or 'inherent' randomness [177]. This is the kind of randomness that annoyed Einstein who supported that "God does not play dice" [179, 181]. Following Einstein's ideas, John Bell produced the experimentally testable 'Bell inequality', the violation of which reveals if God plays dice! [181,182] Below we shall see why this new kind of randomness is useful for technological purposes.

H.1 Classical

H.1.1 Random Numbers and Their Uses

Random numbers are useful in many applications such as cryptography, randomised polling, lotteries, gaming and gambling, industrial testing and labelling, computer simulations of complex physical, chemical, biological, social and economical systems etc [177, 183]. The two types of classical Random Number Generators (RNGs) are the pseudo-RNG and the 'true' RNG [179].
A pseudo-RNG generates numbers algorithmically directly from a computer. However, because digital computers operate deterministically they cannot produce really random numbers. John von Neumann had stated that "Anyone who considers arithmetical methods of producing random digits is, of course, in the state of sin" [183]. Indeed, pseudo-random number sequences suffer from long-range correlations that undermine cryptographic strength and produce errors in Monte Carlo simulations [184].

The 'true' RNG uses some physical process that is hard to predict. Such a complex process can be for example the noise in a thermal, atmospheric, or electrical circuit system [183].

In the cases of both classical and quantum cryptography, the existence of a 'good' RNG is vital. The applications of cryptography to our everyday lives are numerous: online payments, ATMs, e-banking, wireless keys, email access, mobile communications etc [183]. Simply, cryptography is the science of keeping a message secret. The security of a message relies on the production of perfectly random, uncorrelated digits used to encode data. Such a random sequence must be unpredictable for

any adversary wanting to break the code. In particular, in the famous Vernam, B92, BB84 protocols of quantum cryptography the two parties have to produce random numbers either for their keys or for their measurement choices [185, 186]. But if the physical system used to produce random numbers, despite its complexity, is fundamentally deterministic then an eavesdropper can know a more detailed description of that system and thus can, in principle, predict the sequence [177]. Analogous dangers hold in the case of gambling as well. Imagine that a roulette is uncontrollable for you and seems fair, so, you bet your money for a specific 'random' outcome. At the same time, your opponent knows the complete details of the mechanism-motion of the roulette and so knows the outcome in advance.

H.2 Quantum

In contrast, if there are physical procedures intrinsically random then unconditional secure coding schemes and unconditionally fair gaming schemes are doable [177]. A QRNG utilises genuine quantum features to generate random bits. Figure H.1 shows an optical quantum system used to generate random numbers. A single photon is sent towards a semitransparent mirror (beam

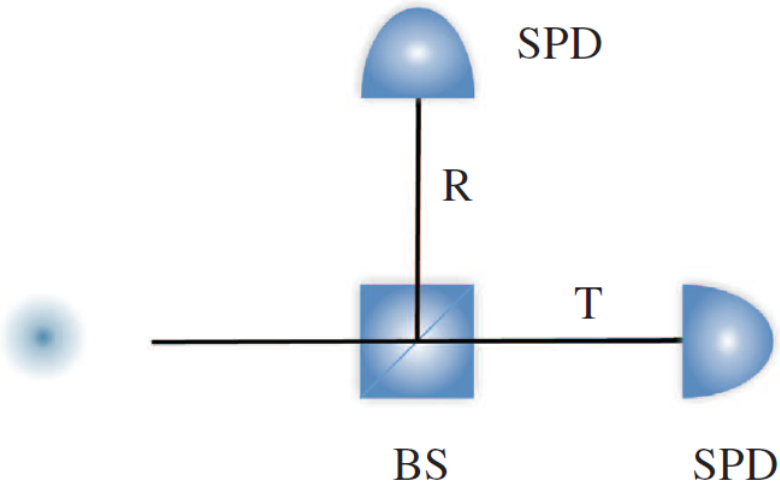


Figure H.1: After passing through the beam splitter (BS) the photon is in a superposition of two paths, the reflected (R) and the transmitted (T) path. A single photon detector (SPD) measures the path information of the photon and so generates a random bit. Image taken from [184].

splitter). The photon can be reflected or transmitted with equal probabilities and this fact is intrinsically random. If we trust the validity of quantum theory [177] and the internal working of the semitransparent mirror [154, 187] we can claim that which detector will click is a fundamentally unpredictable event. This apparatus is one of the commercially popular and successful QRNGs (ID-quantique, [188]).

So far there are many patents for QRNGs available either in the market or online for free use [154].

They use principles of quantum systems such as photon arrival times (PicoQuant [189], Qutools [190]), photon emission in semiconductor LEDs (QBG121 [191]), photon bunching (Whitewood [192]), electron-hole pair generation in a semiconductor (MPD [192]), measurement of quantum noise at high frequencies (Quintessencelabs [193]), measurement of quantum fluctuations of the vacuum (ANU [194]) and shot noise based (Comscire [195]).

Apart from these technologies, it is remarkable that scientists have proposed a QRNG based on accessories almost available in our mobile phones! [196] The quality of the cameras integrated in mobile phones has improved to such an extent that they are sensitive to light at a few-photon level. This sensitivity can be exploited for a construction of a quantum-noise based QRNG. This proposal opens new horizons towards a low cost, small size and user friendly QRNG.

Regarding the randomness verification, there are statistical tests that check one or more properties of long sequences of random numbers. The examined properties can be the serial autocorrelation or the bias which is defined as the difference between the observed probability of zero and the observed probability of one [186]. The crucial point in statistical testing is that if a generator passes all known statistical tests, that does not mean that it is random! It means only that it passes all known randomness tests! [186]

H.3 Discussion

H.3.1 The Device-Independent Approach

Should we believe a RNG if our theories are not the final theories of physics, if an experimental device stops working or degrades or if an adversary has prepared in advance our devices? The research on the super strong nonlocal quantum correlations [182] gives answers to these questions introducing the new field of the device-independent quantum random number generation (DI-QRNG) [197–199]. The device independent approach deals even with the worst imaginable paranoid-minded [154] scenario where a malicious manufacturer has stored a random sequence that passes all the tests into a hard drive and has equipped a 'random number' generator with this hard drive [184]. In that case the adversary knows in advance the sequence and the honest user feels secure because their device passes the statistical tests. In the device-independent approach we confront our experimental devices as black boxes assuming nothing about their internal working [179, 187]. The fact that the input-output statistics of these boxes violate a certain kind of inequalities, the Bell-type inequalities, can certify that the inner working of these black-boxes is fundamentally random [187]. This new field of quantum random number generation utilises the fundamental Valentini's theorem which says that "nonlocal correlations plus determinism implies signalling" [179,200]. No-signalling, which means the impossibility of sending a message faster than light, is an undoubted principle of nature. So, the observation of non-local correlations through a violation of a Bell-type inequality sacrifices determinism and guarantees some amount of randomness. The main idea behind the Device Independent (DI) approach is that the black box output must be random, otherwise some fundamental physical law must have been broken [154]. The DI method promises randomness which

is [177, 179, 201] :

- Certifiable, in the sense that the randomness of the generated numbers is verified through reliable tests;
- Private, in the sense that the random numbers will appear random not only to the honest user but also to any other potentially adversarial user;
- Device independent, in the sense that the production of random numbers does not rely on any modelling of the internal working principles of the experimental devices and thus it is robust to imperfect or malicious devices.

Currently, the efforts for a DI-QRNG are not at a theoretical but an experimental stage [202, 203]. In the upcoming 'quantum at home' era QRNGs will provide unbreakable and secure passwords wherever necessary: in home security systems, strongboxes, transactions, and entertainment and investments with fair gaming and gambling.

I Quantum Money

Money is essential in people's lives. It does not only play an important role nowadays, but it was fundamental along all humanity history, being central in the establishment of trading and thus in the progress of civilisations. But what is money? Money is any item or verifiable record that is generally accepted as payment for goods and services and repayment of debts in a particular place. The main functions of money are distinguished as: a medium of exchange, a unit of account, a store of value, and sometimes a standard of deferred payment. Any item or verifiable record that fulfils these functions can be considered as money. It is historically an emergent market phenomenon establishing a commodity money, therefore we observe items like barley, shells and sugar (later) serving as money by old societies. It was later when the use of gold and silver coins was first introduced. Nowadays nearly all contemporary money systems are based on fiat money. Fiat money, like any check or note of debt, is without use value as a physical commodity, and it derives its value by being declared by a government to be legal tender.

While currencies like the dollar, the euro or the pound are fiat money centralised, controlled and emitted by governments and central banks, the rise of cryptocurrencies lead by the Bitcoin since 2009 is changing the paradigm of trading and the money itself. Unlike the mainstream currencies, cryptocurrencies are digital, decentralised, deflationary money. Because of their novelty and of not being something physical, but rather digital information based on cryptography and not emitted by any bank, they were skeptically received by most people. Nonetheless, cryptocurrencies are finding their way into the international market. At the time of this writing, a single Bitcoin, whose value was less than $0.003 in 2010, is around $4000.

Both these approaches to money have problems, or at least could have in the future. Paper money (unlike gold, silver or the cryptocurrencies) can be forged by people. Government and central banks have been trying to avoid forgery for centuries. On the other hand, the cryptocurrencies (and digital banking in general) are based on classical cryptography. The advent of powerful quantum computers in the future may threaten their system. We shall then explore in which ways the quantum technologies might solve these problems.

I.1 Classical

In the following we briefly review the current (classical) versions of both both paper money and cryptocurrencies, focusing on the latter since is the less familiar concept.

I.1.1 Paper Money

As mentioned above, paper money is a case of fiat money, which is of no value as a physical commodity and it derives its value by government decree. To fulfil its various functions, one requires money to have certain properties:

- Fungibility: its individual units must be capable of mutual substitution (i.e., interchangeability);
- Durability: able to withstand repeated use;
- Portability: easily carried and transported;
- Cognizability: its value must be easily identified;
- Stability of value: its value should not fluctuate;
- Scarcity: there is a moderate quantity of it and it is difficult to obtain;
- Irreplicability: it is hard to counterfeit.

While the first four conditions are obvious and paper money does fulfil them, the last two, especially scarcity, can escape our attention, since paper money does not have these characteristics. We desire irreplicability as a condition to avoid counterfeit by the general public. On the other hand, governments usually print money as one of their principal economic policies. Fiat money needs then to be easy to print by central banks but hard to forge by others. Therefore governments put a substantial effort in developing anti-counterfeiting measures. Traditionally, these measures involve including fine detail with raised intaglio printing on notes which would allow non-experts to easily spot forgeries. On coins, milled or reeded (marked with parallel grooves) edges are used to show that none of the valuable metal has been scraped off. Figure I.1 shows anti-counterfeiting features on a U.S. $20 note.

One also wants money to be scarce, which is somehow linked to irreplicability. Even though it can be hard to create a copy of an object, this same object can be abundant in nature, so the act of simply collecting it could be regarded as forgery. No one would consider taking e.g water as a medium of exchange (even though water does certainly have a cost attributed by the market). Materials which certainly have both scarcity and irreplicability characteristics are gold and silver, and they were used for a long time as a monetary system (the golden standard). Banknotes were actually originally issued by commercial banks, who were legally required to redeem the notes for legal tender (usually gold or silver coin) when presented to the chief cashier of the originating bank.

I.1.2 Cryptocurrencies

A cryptocurrency is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. They are normally decentralised and deflationary money, with Bitcoin becoming the first one in 2009. Since then, numerous cryptocurrencies, frequently called altcoins, have been created.[1]

[1] https://www.coingecko.com

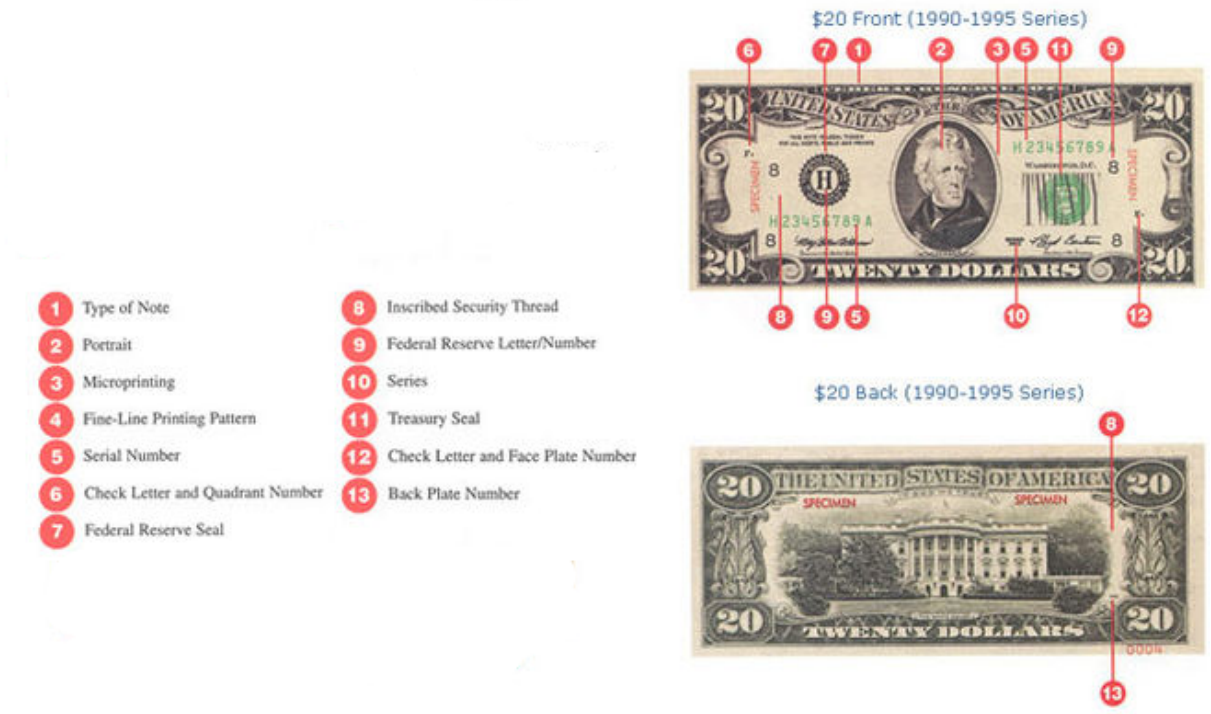


Figure I.1: Anti-counterfeiting features on an old U.S. $20 note. Image taken from [204].

There are several cryptographic technologies that make up the essence of Bitcoin [205]. First is public key cryptography, which is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only by the owner. This accomplishes two functions: authentication, which is when the public key is used to verify that a holder of the paired private key sent the message, and encryption, whereby only the holder of the paired private key can decrypt the message encrypted with the public key. In terms of the Bitcoin framework, each coin is associated with its current owner's public ECDSA (Elliptic Curve Digital Signature Algorithm) key [206, 207]. When you send some bitcoins to someone, you create a message (transaction), attaching the new owner's public key to this amount of coins, and sign it with your private key. When this transaction is broadcast to the bitcoin network, this lets everyone know that the new owner of these coins is the owner of the new key. Your signature on the message verifies for everyone that the message is authentic. The complete history of transactions is kept by everyone, so anyone can verify who is the current owner of any particular group of coins.

This complete record of transactions is kept in the block chain, which is a sequence of records called blocks. All computers in the network have a copy of the block chain, which they keep updated by passing along new blocks to each other. Each block contains a group of transactions that have been sent since the previous block (see figure I.2). In order to preserve the integrity of the block chain, each block in the chain confirms the integrity of the previous one, all the way back to the first one, the genesis block. Record insertion is costly because each block must meet certain requirements that make it difficult to generate a valid block. This way, no party can overwrite previous records

by just forking (splitting) the chain.

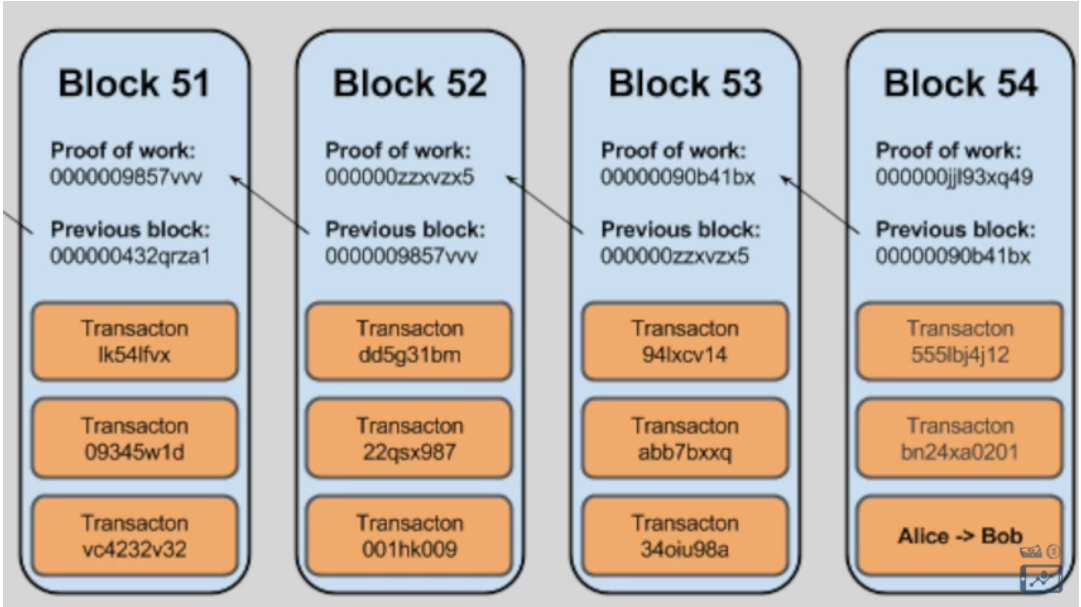


Figure I.2: The block chain and some of its blocks. Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block. Image taken from [208].

To make generating bitcoins difficult the hashcash cost-function is used [209]. Hashcash is the first secure, efficiently verifiable cost-function or proof-of-work function and it is also used to limit email spam and denial-of-service attacks. The idea behind the hashcash is to have an algorithm that requires a selectable amount of work to compute, but the proof can be verified efficiently. In the Bitcoin framework, the hashcash cost-function iterates by perturbing data in the block by a nonce value (32-bit field), until the data in the block hashes to produce an integer below the threshold - which takes a lot of processing power. This low hash value for a block serves as an easily-verifiable proof-of-work - every node on the network can instantly verify that a given block meets the required criteria. If not, it is discarded. The whole integrity, block-chaining, and the hashcash cost-function all use SHA256 as the underlying cryptographic hash function, which is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) [210, 211].

The block chain and the public key cryptography are the main parts of the Bitcoin's functionality. The block chain keeps a record of all transactions, while the cryptography guarantees that these transactions are securely performed. Contrary to what people might believe, there are no actual encrypted pieces of code inside the system named Bitcoins. Also, you do not keep Bitcoins inside your computer. What happens is that a quantity of coins is associated to your private key, and only with this key it is possible to move the associated Bitcoins around the network.

I.2 Quantum

Both banknotes and cryptocurrencies might benefit from quantum technologies in the future: the banknotes from anti-counterfeiting features and cryptocurrencies from improved security features in their underlying cryptography. We describe these possible improvements in the following.

I.2.1 Paper Money

The idea of a proposed design of banknotes which makes them impossible to forge with the use of quantum mechanics was put forward in about 1970 by Stephen Wiesner [212]. His idea, and all the subsequent ones, is based on the no-cloning theorem. The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state. In other words, there is no quantum transformation that takes $|\Psi\rangle|0\rangle \to |\Psi\rangle|\Psi\rangle$ for an unknown state $|\Psi\rangle$, since this transformation is not unitary. By encoding information about the value of the note in a quantum state, it is not possible to duplicate the note.

Wiesner used photons as a system for encoding information. In each note, there is a sequence of quantum states in one of two complementary bases. For example, photons in one of four polarisations could be used: at 0°, 45°, 90° and 135° to some axis, which is referred to as the vertical. Each of these is a two-state system in one of two bases: the horizontal basis has states with polarisations at 0° and 90° to the vertical, and the diagonal basis has states at 45° and 135° to the vertical. By the quantum no-cloning theorem, anyone who does not know the polarisations of these states cannot copy them.

In addition to the physical system, there would be a unique serial number on each banknote, which corresponds to the note's set of polarisations axes. The bank would then store, in a secure location, a database of all the serial numbers together with classical descriptions of the associated quantum state. Thus, whilst the bank can always verify the polarisations by measuring the polarisation of each photon in the correct basis without introducing any disturbance, a would-be counterfeiter ignorant of the bases cannot create a copy of the photon polarisation states, since even if he knows the two bases, if he chooses the wrong one to measure a photon, it will change the polarisation of the photon in the trap, and the forged banknote created will be with this wrong polarisation. For each photon, the would-be counterfeiter has a probability 3/4 of success in duplicating it correctly. If the total number of photons on the bank note is N, a duplicate will have probability $(3/4)^N$ of passing the bank's verification test. If N is large, this probability becomes exponentially small. Hence, these notes are actually more like cheques, since a verification step with the bank is required for each transaction.

Wiesner's scheme has two striking advantages. Firstly, the scheme requires only single coherent qubits and one-qubit measurements; there is no need for any entanglement. For this reason, the scheme might be practical long before universal quantum computing. Secondly, the security of the scheme is information-theoretic guaranteed by the laws of quantum physics, rather than computational. On the other hand, Wiesner's scheme requires a giant secret database maintained by the

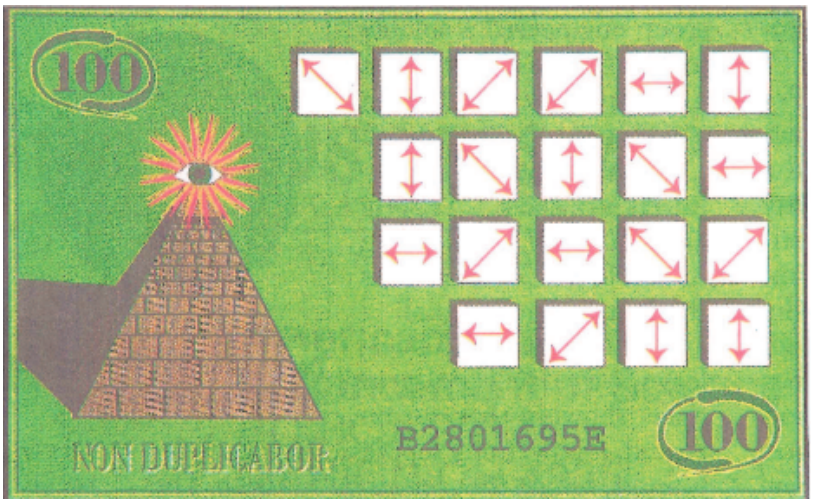


Figure I.3: An illustrative quantum note. In each note, there is a sequence of quantum states in one of two complementary bases. Image taken from [213].

bank. But in 1982, Bennet, Brassard, Breidbart and Wiesner (BBBW) showed how to avoid the giant database, at the cost of making the security of the quantum money computational rather than information-theoretic [214]. In modern terms, their proposal was as follows. The bank fixes, once and for all, a secret random seed s. It then distributes banknotes, each of the form $|y\rangle|\psi_{g_s(y)}\rangle$, where $y \in \{0,1\}^n$ is a unique serial number for the banknote, $g_s : \{0,1\}^n \to \{0,1\}^n$ is a pseudorandom function, and $|\psi_{g_s(y)}\rangle$ is the state obtained by starting from $g_s(y)$, grouping the n bits into $n/2$ blocks of two, and mapping each 00 to $|0\rangle$, 01 to $|1\rangle$, 10 to $|+\rangle$ and 11 to $|-\rangle$. Using its knowledge of s, the bank can verify the authenticity of any note $|y\rangle|\psi_{g_s(y)}\rangle$ by computing $g_s(y)$ and then measuring each qubit of $|y\rangle|\psi_{g_s(y)}\rangle$ in the appropriate basis.

However, the BBBW scheme still has a serious drawback: s must remain a closely-guarded secret. It led Scott Aaronson to ask if there exist quantum money states that anyone can verify - that is, for which the authentication procedure is completely public - but that are still unfeasible to copy [213, 215]. He then proposed a candidate proposal based on random stabiliser states. A stabiliser state is a pure state that can be obtained by starting from $|0\rangle^{\otimes n}$ and then applying controlled-NOT, Hadamard, and $\pi/4$-phase gates. By applying these gates randomly, one obtains interesting quantum states called quantum t-designs. We refer the reader to [216, 217] for more information on t-designs. In figure I.4, we summarise some of the proposals for quantum schemes for quantum money.

I.2.2 Cryptocurrencies

As explained before, cryptography is central in the cryptocurrencies' functionality, especially for Bitcoin. This is how cryptocurrencies maintain their security. With a possible advent of powerful quantum computers, classical cryptography in general could be threatened, and therefore, so can cryptocurrencies' security. It is then natural to ask if Bitcoin and other altcoins can benefit from

Money Scheme	Type	Oracle	Security	States Used
Wiesner	Private-key	Random	Unconditional	Single qubits
BBBW	Private-key	None	Assuming PRFs	Single qubits
Modified Wiesner	Query-secure	Random	Unconditional	Haar-random
Modified BBBW	Query-secure	None	Assuming PRFs	Haar-random
Quantum Oracle	Public-key	Quantum	Unconditional	Haar-random
Random Stabilizers	Public-key	None	Conjectured	Stabilizer
Matrix Product States	Public-key	None	Conjectured	MPS

Figure I.4: Some of the proposals quantum money could be based on. Wiesner is from [212], BBBW is from [214] and the others are from [215]. Table taken from [215].

quantum cryptography. Since the Bitcoin uses public key cryptography, it could use some of the various protocols of QKD, e.g. the BB84 or the E91 protocol. We refer the reader to Article F for an explanation on the BB84 protocol.

Another feature central to cryptocurrencies is the set of hash functions. As previously mentioned, hash functions are designed to take a string of large length (theoretically any length) as an input and produce a short (in practice a fixed-length) hash value. This allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it (or equivalent alternatives) by knowing the stored hash value. There are already proposals for quantum hash functions, something Bitcoin can take advantage of in the future. One simple example of a hash function is to encode a word $w \in \{0,1\}^n$ in a single qubit like [218]

$$\psi : w \to \cos\left(\frac{2\pi w}{2^n}\right)|0\rangle + \sin\left(\frac{2\pi w}{2^n}\right)|1\rangle,$$

where $w = w_0 ... w_{n-1}$ is treated as a number $w = w_0 + w_1 2^1 + ... + w_{n-1} 2^{n-1}$. Clearly, we have that ψ has the one-way property, since we cannot learn about w from ψ.

An interesting proposal for a quantum hash function is based on quantum walks [219]. The basic discrete quantum walk includes two quantum systems: walker and coin. The motion of the walk is conditioned by the coin state, which in turn is flipped by a fixed coin operator after every step. The resulting probability distribution relies on only the initial coin state and the step number. Suppose the coin operator at each step depends on a binary string, i.e., message. The input of the constructed quantum hash function is a binary string, i.e., the message, and the resulting probability distribution is used as the output hash value. The coin state is the control parameter so the constructed quantum hash function is a keyed one. The nth bit of the message controls the nth step of the walk.

Another hashing scheme using t-designs was put forward by Scott Aaronson in the same paper in which he proposed the use of random stabiliser states as possible candidates for quantum money [215]. It uses a pseudorandom generator g, and given the secret key s, one first computes $g(s)$ and then reinterprets $g(s)$ as a description of a quantum circuit $U_{g(s)}$ over some universal basis of gates, which acts on m qubits. Given $|\psi_s\rangle = U_{g(s)}|0\rangle^{\otimes n}$, another person can measure the state $U^{-1}_{g(s)}|\psi_s\rangle$ and then check whether the outcome is $|0\rangle^{\otimes n}$, without ever knowing about s.

I.3 Discussion

The use of quantum technologies could have an impact on the future of money, both in the way we design our banknotes and also in emerging technologies based on cryptography such as the cryptocurrencies like the Bitcoin. One of the challenges to substitute usual paper money by quantum systems like photons in a way to avoid forgery is the fragility of quantum systems themselves. We use mostly paper or plastic as notes because of their practicality and general resistance in everyday use. Having stored photons in our wallets which can maintain their information and coherence after months and years of usage is a monumental challenge. We also need to take into account the cost of producing these notes. It would not make sense from an economic point of view to try to substitute a $1 note by a quantum money note with the same value, but which costed $1000 or more to produce. The use of quantum money could then be feasible if these quantum systems are to be cheaply produced or if they are used as high value notes or credit cards.

The application of quantum cryptography to cryptocurrencies seems more straightforward, since it would only be a matter of modifying the usual classical cryptography to a quantum one. The QKD technology is already being applied by various companies, e.g. MagiQ Technologies, ID Quantique, QuintessenceLabs and SeQureNet. The implementation of quantum hash functions will probably take longer to be commercialised. However, since there are no quantum computers around to threaten the classical cryptography, there is little point in implementing quantum changes into the cryptocurrencies's functionality. This leads to the question of whether the quantum security protocols are going to be cheaper, or at least comparable in price to classical protocols and hashing functions. In order to operate the quantum protocol, a large computational power needs to continuously verify coin transfers and write them in the block chain, and the benefit for this must outweigh the cost, electrical and otherwise.

J Facial Recognition

There are many problems that computers are much better or faster than humans at solving. However, there are certain problems that humans easily outperform even the most powerful of computers. One example is facial recognition. Humans can recognise faces, even if they are in shadow, smiling or frowning, or wearing makeup. For computers, however, facial recognition is an intractable problem and even heuristic algorithms are computationally expensive and often inaccurate. Researchers in this field have taken inspiration from the human brain, which performs facial recognition so efficiently, to create algorithms for computers based on neural networks [220–222].

Facial recognition is a well-established area of research, with systems currently used in numerous places in everyday life: epassport gates in airports, identifying criminals from CCTV footage, and unlocking mobile phones. However, facial recognition could be used even more to improve our safety and security – from picking out known criminals in a crowd at events, or locating lost children, to checking identities at ATMs. At the moment, facial recognition suffers from problems due to poor lighting, occlusions due to eg. glasses, makeup, or hair, different facial expressions, and different angles to the camera. Clearly these are likely to occur in many situations where facial recognition could be used. Even under perfect conditions such as epassport gates matching you to your passport photograph (bright lighting, neutral expression, looking at the camera etc.), the current technology is not infallible, with manual matching between camera and passport photos to ensure security at borders. Of course different applications of facial recognition have different requirements from its technology. Airports can assume bright lighting, no occlusions, and neutral facial expressions because passengers can be asked to comply to pass through border control. However, matching criminals caught on camera will usually have to deal with poor resolution and lighting, face being partially turned away from camera and possible occlusions. Also, software should be robust against attempts to fool it called 'spoofing'; for example holding a photograph of the person up to the camera needs to be rejected for applications where individuals scan their faces privately for access purposes. There exist many algorithms for facial recognition and some are better at dealing with imperfect conditions, others for detecting spoofs and others are more efficient for real-time matching. Unfortunately, none of them are perfect for the applications and much research is still being done on how to improve them. Here, we look at how quantum machine learning could improve the field.

J.1 Classical

For facial recognition algorithms, the aim is to translate information in an image of a face into a manageable and useful format such that the person's identity can be verified or found from a database. There are three main steps involved in facial recognition:

- Face detection - locating a face in an image;
- Feature extraction - extracting the important features and reducing dimensionality;

- Face recognition - matching the face to one in the database, using a classification algorithm.

In this report, however, we focus on the dimensionality reduction and classification parts. Assuming a face has been located in an image, it can been converted into a matrix by representing each pixel as a number in a matrix corresponding to its intensity or colour. However, if your image is 476x476 pixels, your matrix will be $476^2 = 226576$ dimensional, which is a lot of data to store and will make the matching process very slow if your system is able to handle that amount of data at all. This is why an important part of facial recognition algorithms is a dimensionality reduction process. Once the data of an image has been extracted, it is compared to all the faces in the database and determined which one it is closest to by some measure. There are many algorithms for dimensionality reduction and classification, but we will just cover a few of them here.

J.1.1 Dimensionality Reduction

First, we look at dimensionality reduction. This can be done by determining a basis such that the important information is contained in a linear combination of fewer basis elements than the dimension. There are many algorithms designed to do this and each one has its own basis. The algorithms can be broadly categorised depending on the basis elements as either holistic (each basis element considers the whole face) or feature-based (each basis element considers a feature, such as eyes, nose or jawline). There is evidence to suggest that feature-based algorithms outperform holistic ones [223]. However, the most common algorithms are Principal Component Analysis (PCA) [224] and Linear Discriminant Analysis (LDA) [225], which are both holistic. Other notable algorithms are Vector Quantisation (VQ) [226], which is also holistic and Non-negative Matrix Factorisation (NMF) [226], which is feature-based.

There are two main ways of achieving dimensionality reduction and keeping the important information:

1. Approximating the data matrix in such a way that the information lost is minimised;
2. Choosing information to keep such that data for the same face is very similar but different to any other face.

If the image needed to be reconstructed, the first method would be preferable, but if you only needed to validate or match a face from a database, either could be used. The aim of any dimensionality reduction algorithm is to find the coefficients and basis elements that minimise the information lost when making an approximation to the data matrix or that maximises the distance between different faces, but minimises the distance between images of the same face. These optimisation problems are generally solved using machine learning.

J.1.2 Machine Learning

Machine learning is a vast and well developed field of research. Briefly, machine learning does not follow predetermined rules, but uses data to learn which rules optimise the outcome. The phase in which the system learns is called training and the data it uses is the training data. There are two main types of training - supervised and unsupervised. In unsupervised algorithms, the system must determine a function to describe the problem using unlabelled training data such that it is not classed as correct or incorrect. In supervised algorithms, the data used is labelled and so the desired output is known. Supervised algorithms maximise the class discrimination and unsupervised algorithms minimise the information loss.

The unsupervised algorithms (eg. PCA, VQ, NMF) approximate the data matrix as a linear combination of basis elements. Equivalently, it can be formulated as $V \approx WH$, where the matrix V holds all the data of the face, the columns of W are the basis elements and the columns of H give the weighting of the corresponding basis vectors. This can be seen by taking the sub-problem $v \approx Wh$, where v is a column in V and h is the corresponding column in H [227]. Wh can be written equivalently as $\sum_{i=1}^{n} h_i W_i$, where n is the dimension of the vectors, h_i is the ith element in vector h, and W_i is the ith vector in matrix W. Not only is this a compact notation, but importantly if V is an $n \times m$ matrix, W is an $n \times r$ matrix and H is an $r \times m$ matrix. This means r can be chosen to be much smaller than n and m and this reduces the dimensionality of the problem and hence reduces the computational complexity of the classification algorithm.

The differences between the algorithms are the constraints placed on the matrices W and H. These constraints are what control the basis used. PCA requires the columns of W to be orthogonal and the rows of H to be orthogonal to each other, VQ needs each column of H to contain precisely one 1 and NMF restricts all three matrices to be non-negative (ie. all elements are non-negative) [226]. Once the data is collected into a matrix and the constraints have been decided, the problem becomes finding the factors W and H. The general idea is to iteratively improve the values such that the error or distance between V and WH is minimised.

PCA prioritises showing the maximum variation in data. For example, data on a straight line in two dimensions is normally described by two coordinates, however clearly this could be described by one coordinate if the basis is a vector along that line. This is shown in figure J.1 where the most variation is given by the first principal component. PCA determines which basis should be used to maximise the information about all the data if one vector is discarded. This is extendable to higher dimensions and the basis vectors used in face recognition are called 'eigenfaces'. The data for faces will be very similar, so a lot of the information will not help distinguish faces and so PCA determines which data give the most variation between faces and hence are the most important.

The supervised algorithms (eg. LDA) maximise the distance between classes - ie. wants data to give big differences between different faces and small differences for images of the same face. This can be seen in figure J.2 where the chosen line they are projected onto separates out the different classes more. To be more precise LDA maximises the ratio between the determinant of the between-class scatter matrix and the determinant of the within-class scatter matrix. The between-class scatter

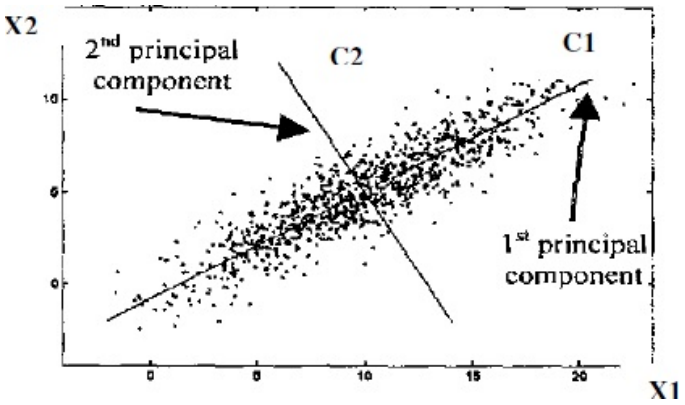


Figure J.1: Graph showing principal components of a data set with two classes. Taken from [228].

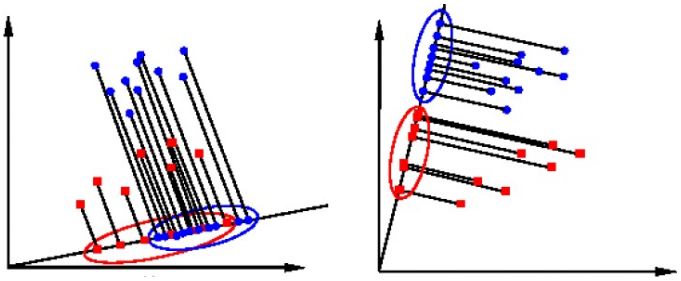


Figure J.2: Graph showing data of two classes projected onto different vectors. Taken from [228].

matrix is given by [225]

$$S_B = \sum_{i=1}^{c} N_i(\mu_i - \mu)(\mu_i - \mu)^T, \tag{3}$$

and the within-class scatter matrix is

$$S_W = \sum_{i=1}^{c} \sum_{x_k \in x_i} (x_k - \mu_i)(x_k - \mu_i)^T, \tag{4}$$

where μ is the average vector over all tested images, μ_i is the average vector over all images from class i, N_i is the number of samples in class i and x_i is a single data point. The basis vectors used in LDA are called 'Fisherfaces'. The main difference between PCA and LDA is that PCA maximises the variation between all data, including images of the same face, whereas LDA maximises the variation only between images of different faces. This means that LDA is less sensitive to variations in lighting and facial expression because it aims to minimise the variations for the same face whereas PCA will maximise it and the differences due to lighting and facial expression are generally a lot bigger than between different people under the same lighting with the same expression.

J.1.3 Classification

Once the training data has been used to determine the optimal space to be used, a new face is projected onto this space and the resulting coefficients are used to classify it (say which person in the database it is). As the data is unlikely to exactly match that in the database, there needs to be a way of defining which person it is 'closest' to. One of the most common ways of classification is to minimise the Euclidean distance between the vector describing this face and the mean vector describing each person, where the vectors are made by stacking the columns of the matrix H. Another distance metric is the l_1 norm. Also correlation coefficients may be used. However, it is usually more accurate to use learning algorithms to determine the best classification using all the data points (not just the mean value). This can be done using the K-Nearest Neighbour (KNN) algorithm [229], or support vector machines [230].

Another popular method for facial recognition are Artificial Neural Networks (ANNs). This is inspired by the biological processes in our brains. ANN performs the dimensionality reduction and/or classification task. Briefly, ANNs use layers of nodes that connect to form a directed, weighted graph. Each node, or neuron, takes input from the previous layer, performs a non-linear summing operation on that input and gives an output to the next layer. A popular ANN used for facial recognition is a self-organising map [231], which performs dimensionality reduction and can be considered as a non-linear version of PCA. In this, a multidimensional space (input layer) is mapped to a discrete array of a 2D lattice (computational layer). The lattice is initially assigned values at random. For every input data, the node nearest (least Euclidean distance) and connecting nodes are adapted so that they are closer to the input weight. This is repeated until the nodes become stable and so map onto the input states. A similar ANN is learning vector quantisation [232].

Each method has its own advantages and disadvantages and some perform better under certain conditions. There have been many comparisons between different algorithms in different conditions eg.between NMF and PCA [233] which also compares different metrics used for classification. For each application, all the algorithms should be compared to discover which is the most appropriate. Due to the importance of identity verification/matching for security purposes, the accuracy is extremely important which is why new methods are constantly been considered. In the following section we look at how quantum physics may improve facial recognition.

J.2 Quantum

Quantum Machine Learning (QML) [234] is a recent field emerging from the inclusion of quantum principles in machine learning. Quantum computing could help machine learning by performing algorithms intractable for classical computers or provide a considerable speedup. This means that the number of training data required and the time required to perform the optimisation task could be reduced. Also, quantum principles could be used to invent new algorithms which would converge on a more accurate optimisation. The inclusion of quantum physics in machine learning is shown clearly in figure J.3.

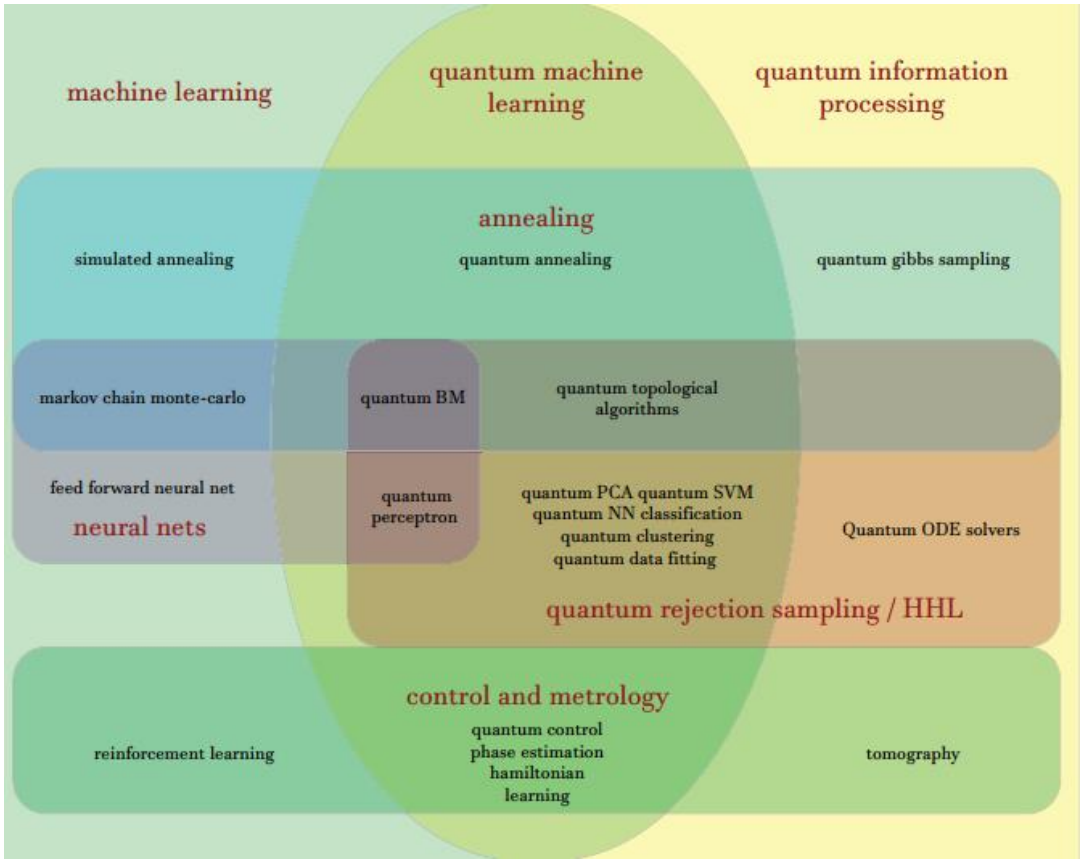


Figure J.3: Diagram showing the overlap of quantum machine learning with classical machine learning. Image taken from [234].

J.2.1 Quantum Annealing for Matrix Factorisation

Universal quantum computers are yet to be realised, but D-Wave have demonstrated quantum speedup using their adiabatic quantum annealers. Therefore, a promising near-future quantum algorithm would use D-Wave's hardware. They have proposed a method that uses their quantum annealers for matrix factorisation [235]. This method, non-negative/binary matrix factorisation, can be thought of as somewhere between NMF and VQ and is a holistic algorithm. The constraints for this are that W should be non-negative ($W_{ij} \geq 0$) and H should be binary ($H_{ij} = \{0, 1\}$). An alternating least squares algorithm is used to find W and H. This algorithm is as follows:

1. Input V and r;
2. Initialise H with each element randomly 0 or 1;
3. While not converged,

$$W = arg(min_{X \in R^{+n \times k}} \|X - VH\|_F + \alpha \|X\|_F); \tag{5}$$

$$H = arg(min_{X \in \{0,1\}^{k \times m}} \|V - WX\|_F); \tag{6}$$

   end while;
4. Output W and H.

Here, we will focus on solving equation (6). This is an optimisation problem involving km binary variables, which for large m is computationally expensive. However, similarly to before, we can note that the ith column of $V - WX$ only depends on the ith column of V and X. Hence we can equation 6 with km binary variables to m optimisation problems with k binary variables each:

$$H_i = arg(min_{X \in \{0,1\}^k} \|V_i - WX_i\|_2), \tag{7}$$

where H_i, V_i and X_i denote the ith column of H, V and X respectively. Each of these optimisation problems has a reduced complexity and can now be performed on a D-wave machine efficiently. The only thing that remains is to convert it to the format that D-wave machines can solve - quadratic, unconstrained, binary optimisation. This is given in detail in [235].

J.2.2 Other Quantum Enhanced Algorithms

The above is a novel algorithm derived from quantum machine learning, designed to be executed by a quantum annealer, however the speedup from replacing parts of existing classical algorithms with a quantum counterpart could also be beneficial. Quantum versions have been proposed for the following algorithms: PCA [236], Support Vector Machine (SVM) [237], ANN [238] and a classification based on KNN [239]. These all require a universal quantum computer, and so cannot be a near-future alternative. Perhaps the most interesting of these is the classification. The idea is to create a superposition of the training data vectors such that the coefficients contain the

information about the distance between the input vector and each corresponding training vector. At the moment, there is no significant speedup observed but there is promise that with some improvements the algorithm's time complexity could be independent of the number of training vectors.

J.3 Discussion

D-wave have presented a method of facial recognition that uses their quantum hardware for one optimisation task and outperforms two classical algorithms that they compare it to. However, it is noted that this does not mean it outperforms all classical equivalents for that algorithm or all other methods (eg. PCA, LDA, NMF). In fact, it is suggested that a classical heuristic algorithm would outperform this quantum annealing version. However, classical optimisation is a topic that has been thoroughly researched and well developed, and it is promising that D-wave's third generation chip is already competitive. This is a very recent result and this technology would benefit from more analysis, particularly looking at whether it could be useful under certain conditions (poor lighting, resolution, occlusions etc). Further testing and analysis will help determine whether quantum computers will improve the efficiency and accuracy of facial recognition and hence be implemented in everyday security.

Although this article has focused on facial recognition, pattern recognition occurs in many areas of life for which machine learning is already implemented and therefore quantum machine learning could be useful too. One example is spam filtering. The best current filters use machine learning algorithms [240, 241]. The overall process is very similar to facial recognition:

1. Convert message into useful format;
2. Dimensionality reduction - keep only important data;
3. Classification - decide whether the message is spam or not.

The main difference is that the classification is binary - either it is spam or it isn't - as opposed to finding the closest match to a face in a database. The individual stages are very different too as converting a message into a useful format is less obvious. During dimensionality reduction words that commonly occur in all emails (an, the, it) are ignored and only the parts useful for determining the difference between spam and not spam are kept. Machine learning techniques for spam filtering are young and quantum machine learning has not been considered in this application yet. However, with the increasing amount of data sent in emails and particularly the rising number of spam messages the need for handling large quantities of data quickly is increasing and the principals are transferable. It seems likely that quantum computers won't be filtering your emails anytime soon, but it is certainly a possibility for the future.

K Solar Cells

Inefficiencies in the energy conversion of current solar cell technology are a large barrier to our ability to rely on this renewable energy source for a significant proportion of our power consumption. These inefficiencies are primarily a result of fluctuations in the light received by the photocell [242], and therefore it is important to consider how quantum technologies could be used to increase photocell efficiencies by suppressing these fluctuations. In fact, Quantum Heat Engine (QHE) photocells that consist of two photon absorbing channels have theoretically been shown to suppress light fluctuations, and this energy regulation increases the efficiency of energy conversion from solar energy incident on the photocell to electronic energy produced [243]. These can be made from quantum dots, which have already demonstrated promising results for increasing the efficiency of light harvesting [244].

K.1 Classical

K.1.1 A Comparison of Classical and Quantum Photovoltaics

Thermodynamic heat engines extract power from the flow of energy between a hot and a cold reservoir. The key difference in the case of a QHE is that the flow of energy is between a quantised energy level and a thermal reservoir [245]. QHE photocells can be formed by coupling two nanoscale semiconductors with an electronic state transition, such that the absorption of a single photon by the semiconductor creates some electronic energy [246, 247]. Classical solar technology also utilises semiconductor material linked by a bandgap such that individual photons are absorbed, producing photoelectrons [248]. However, QHE photocells are distinct from classical photocells because in the quantum case the bandgap is formed from two individual quantum states of different energy rather than two materials of different Fermi levels. In classical solar technology, active electronic switching devices such as metal-oxide-semiconductor field effect transistors are used to suppress voltage fluctuations, and this can be combined with techniques to regulate the energy flow by matching the input power to the optimal output power [242]. This requires voltage converters and feedback controllers between the solar panel and the battery, and is necessary to avoid the accumulation and subsequent dissipation of excess energy. In the case of QHE photocells, the energy regulation is possible without requiring such feedback control mechanisms, and is achieved by optimising the internal electronic transition probabilities characterising the QHE photocell [243].

K.2 Quantum

A QHE photocell can be formed from quantum dots, which are nanoscale regions of semiconductor that confine individual energy levels in three dimensions [249]. These structures have been shown to have optimal properties for light harvesting, enhancing the quantum efficiency and electron transport properties that can be achieved [250]. However, the certified power conversion efficiency

of quantum dot based solar cells is still only around a quarter of the efficiency of the most recent classical solar technology [251, 252]. A QHE structure is desired that simultaneously matches the input solar power as close as possible to the average output power required to do useful work, and suppresses energy fluctuations to avoid the accumulation of excess energy. A design which achieves these two optimisation conditions is a QHE photocell consisting of two photon-absorbing channels. One channel absorbs light at a wavelength for which the average input power is high, and the other channel absorbs at a wavelength with low average input power. The photocell switches stochastically between these two channels to convert varying incident powers of light into an approximately constant output. In order to obtain a quantum advantage with this naturally energy regulating mechanism, it is necessary for the difference between high and low input power to be large, such that power fluctuations can be suppressed. It has been shown that this difference is smallest for green light when considering the light incident on Earth's surface, and therefore the absorption of green light should be avoided [243].

In order to describe the power transfer and fluctuations of such a two channel photocell proposed in [243], we can consider that the two input channels a and b which absorb photons with energies E_a and E_b also absorb two different powers $u_a < u_b$. These channels are coupled by the transfer of electrons to the same output state with a lower energy, such that the energy difference in the 'machine' E_M is used to generate electronic power. Therefore, electrons excited by photons from the ground state $|g\rangle$ to an excited state $|a\rangle$ or $|b\rangle$ are transferred to the state $|x\rangle$, losing energy to phonons. This decay to state $|x\rangle$ is possible because fast charge transfer to the machine, governed by rates γ_a and γ_b, dominates over radiative recombination. From state $|x\rangle$ the energetic electrons in the machine can be used to generate electronic power $u_M = E_M\Gamma$ at a rate Γ causing them to decay to a low energy state $|y\rangle$ and eventually the ground state $|g\rangle$ at a rate γ_g. This process is illustrated in figure K.1.

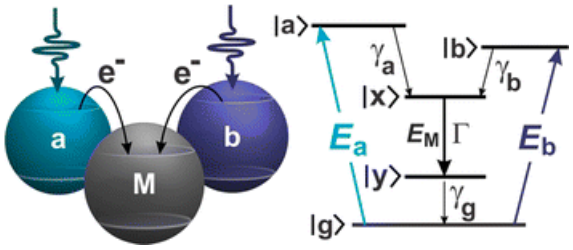


Figure K.1: (Left) Schematic of a two-channel quantum photocell. Photons absorbed by channel a and b give rise to a pair of photoelectrons, generating electronic power in the machine M. (Right) Energy level diagram of the two-channel quantum photocell. E_a and E_b are the excitation energies of the channels a and b with transition rates to the machine M given by γ_a and γ_b respectively. The output energy is given by E_M and is characterised by the rate of relaxation Γ from state $|x\rangle$ to state $|y\rangle$. γ_g represents the rate of decay to the ground state $|g\rangle$. Image taken from [243].

The ratio E_i/E_M is similar for $i = a, b$ which means that neither channel is energetically favoured. In terms of the number of photons absorbed in each channel per unit time, N_a and N_b, the input power from each channel is defined as $u_i = N_i E_i$ for $i = a, b$, and the output power from the machine is $u_M = N_M E_M$, where N_M is the rate of photons extracted from the machine. The photocell can be modelled by discretising time and considering the energy at a time step n to be

given by the sum $\sum_{m<n} u_M$, and the mean and variance of this value can be given by the Central Limit Theorem. The variance can also be derived analytically by assuming that the average power output is given by the machine power $u_M = p_a u_a + p_b u_b$, where p_a and p_b are the respective probabilities of each channel in the photocell absorbing a photon. The variance is then given by $\sigma = p_a (u_a - u_a)^2 + p_b (u_b - u_M)^2 + (1 - p_a - p_b) u_M^2$ from the definition $Var(x) = \sum_i \left[p_i (x_i - \mu)^2 \right]$, with μ being the average value of x. The value of this variance represents the power fluctuations, and can be minimised by a particular choice of photocell parameter u_i/u_M. Also, by considering a light source of wavelength λ and temperature T to be described by an irradiance spectrum $I(\lambda, T)$, the average input energy flux can be written as $u_i = \int A_i(\lambda) I(\lambda, T) \, \mathrm{d}\lambda$, where $A_i(\lambda)$ is the absorption spectrum for the channel. Then the spectral characteristics of the two absorbers can be analysed such that the photocell minimises fluctuations over the largest amplitude of incident energy flux. A key condition found to minimise the power fluctuations is that the output powers must obey the relation $u_a < u_M < u_b$. It is assumed that the channels have unity absorbance and are exposed to a fluctuating light source. Also, to give maximum energy conversion efficiency, they must optimally couple the photon energy into a steady-state output, while minimising fluctuations. These conditions are optimally satisfied by maximising $u_a - u_b$, and by switching stochastically between two on states absorbing high-power u_a or low power u_b. It was found that for absorption in the blue and red regions of the solar spectrum, power fluctuations of the two-channel photocell are always less than those of a one-channel photocell. However, in the green region of the solar spectrum of incident light, the two-channel design shows no benefit and therefore the efficiency is optimised if green light is not absorbed. It is therefore interesting to consider whether plants utilise similar quantum control of light to optimise light harvesting.

K.2.1 Nature-inspired Quantum Alternatives

Despite the promising design for a quantum photocell described here, there also exist more biology-inspired suggestions for organic photovoltaic devices which take advantage of quantum coherence effects similar to those observed in biological photosynthetic systems [253,254]. Such systems would use materials which enable a more delocalised electron wavefunction to increase transport lengths, and therefore aid the efficiency of transporting energy in such light-harvesting systems. This scheme provides an advantage over traditional photovoltaic technology because excellent charge diffusion is possible without reliance on an additional electric field within the active layer. This enables a sufficient directional flow of current without the requirement of additional power to the device. Controlling coherence using organic photovoltaics could therefore be an alternative strategy to utilise quantum effects to increase the efficiency of solar cells, and should be considered alongside the quantum heat engine design discussed above.

K.3 Discussion

While ideas for quantum photocells based on quantum coherence in organic photovoltaics have shown some promising results [255], semiconductor nanostructures in the form of quantum dots have already been shown to be promising candidates for light harvesting, demonstrating external quantum efficiencies exceeding 100% [256]. This is possible because a single high energy photon can produce multiple electron-hole pairs in quantum dots, and a peak quantum efficiency of 114% has been shown with these devices. However, the maximum overall power conversion efficiency using quantum dot solar cells is only 11.6% [251], which is significantly lower than the classical record of 46% [252], and this is due to the low absorption of a monolayer of quantum dots. Approaches to increase this absorption value mainly rely on increasing the surface density of quantum dots and engineering light trapping techniques [257]. By engineering quantum dots with higher absorption and by electronic coupling of quantum dots, the increased power conversion efficiency as a result of the high quantum efficiency and using two-channel quantum heat engines could be harnessed. If this is achieved, quantum dot based solar cells could become the optimal choice for photovoltaic technology.

L Quantum Battery

Batteries are an essential resource in our lives. They are everywhere: smartphones, laptops, cars, smoke detectors, satellites and even sometimes inside people. Since 1800, when Alessandro Volta published the invention of the first battery (called voltaic pile), batteries have determined the evolution pace of some technological areas.

Batteries come in many shapes and sizes. Also, the materials used to fabricate the anodes, cathodes and the medium that provides the ion transport inside them have been changing over the years improving their performance. The voltaic pile, built more than 200 years ago, consisted of a pile of pairs of copper and zinc discs, separated by a piece of cloth moistened with brine [258]. Nowadays the battery market is based in alkaline, lead-acid, and lithium-ion batteries and rapidly changing into an exclusively rechargeable battery market.

The development of low-cost lithium-ion batteries with high energy storage capacity has been crucial for the emergence of new technologies. For instance, in 2008, analysts estimated that lithium-ion battery packs costed $\$600 - \$1,200$ per kWh, but this range would drop to $\$500 - \$800$ per kWh over the following four years. Soon battery packs will cost closer to \$100 per kWh. This means, for instance, that if they are used in electric cars, they will be essentially cheaper than all petrol- and diesel-powered vehicles [259].

L.1 Classical

Despite the battery industry moving between materials and technology schemes over time, they all share the same fundamental principle: batteries are physical systems that store chemical potential energy and let us, on demand, extract directly electrical energy that we use to do work. How can our understanding and control of quantum systems help us to improve batteries?

In general, classical heat engines produce work by operating between a high temperature energy source and a low temperature entropy sink. A quantum heat engine has no cooler reservoir acting as a sink of entropy but has, instead, an internal reservoir of quantum information (or negentropy i.e, negative entropy, a concept introduced by Schrodinger in his book [260]) which allows extraction of work from one thermal bath. If one has a d-level system in a pure state ψ one can draw $kTln\,(d)$ work out of a heat bath of temperature T. If a state of the system is a mixed state ρ, then the amount of work would correspond to

$$W = kTln(d) - TS(\rho), \tag{8}$$

where $S\,(\rho) = ks\,(\rho)$, $s\,(\rho)$ is von Neumann entropy and k is the Boltzmann constant [261]. The equivalence between work and information opened a new way of thinking about the thermodynamics of quantum systems.

L.2 Quantum

A quantum battery could be seen as a small quantum mechanical system that is used to temporarily store energy to transfer it from a production to a consumption centre. Instead of coupling this quantum system to external thermal baths in order to drive thermodynamical engines, we could address it by controlling its dynamics by external time dependent fields. Allahverdyan and colleagues described the maximum extractable work compatible with quantum mechanics, i.e. unitarily, in terms of the density matrix of the system ρ and the internal Hamiltonian H [262]. This quantity called ergotropy is given by

$$W_{max} = \mathrm{tr}\left(\rho H\right) - min\left[tr\left(U\rho U^{\dagger}H\right)\right], \tag{9}$$

where U is the time ordered exponential of the total Hamiltonian (including the time dependent field $V\left(t\right)$) defined as

$$U(\tau) = \exp\left(-i\int_0^{\tau}\mathrm{ds}\left[H + V(s)\right]\right). \tag{10}$$

This unitary transformation determines the evolution of the system. Note that by a proper choice of the field $V\left(t\right)$, any unitary U can be obtained. The minimum in equation (9) is taken over all unitary transformations of the Hilbert space.

Some years after the work of Allahverdyan et. al., this paradigm of unitary work extraction was extended to scenarios where multi-partite systems are considered. Alicky and Fannes showed that the extractable work can be increased by allowing entangling operations [263].

In a complementary way, the problem of charging a quantum battery has been also addressed. The problem of charging a quantum battery in a finite time has been studied in [264] and bounds for an achievable quantum advantage using entanglement in multi-partite systems have been found [265].

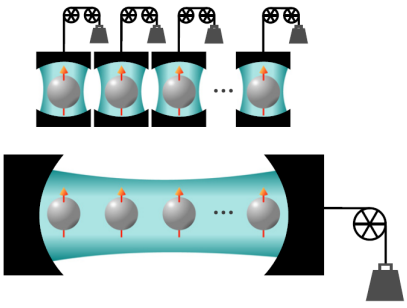


Figure L.1: An array of qubits that represent a quantum battery. They can either be driven in parallel or globally to extract work from them or charge them. It is shown that the correlations between the qubits affect the charging power when the system is driven globally. Image taken from [264].

L.3 Discussion

Although many of these results in quantum thermodynamics are only useful for the understanding of how quantum theory and thermodynamics are related, proving that thermodynamic processes can indeed benefit from collective quantum effects is an exciting achievement, not only for theorists, but also for the big community of scientists trying to implement quantum technologies. Ideally, the processes of reversible energy extraction and charging could be then governed by the system dynamics plus some fields that are only turned on during a certain time interval allowing us to have control over the quantum state of, say, the reactants inside the batteries providing us a new generation of batteries.

M Gravity Sensors

The field of sensing technologies is encompassed by the definition of devices that measure some physical quantity. The efficacy and applications of such devices are determined by the cost, precision/sensitivity and accuracy. Depending on the field of application these variables may exist under different constraints; for example in commercial applications like gravity sensing for oil exploitation a user might accept increased cost for higher precision and accuracy.

Gravity sensing technologies measure the magnitude of acceleration due to some gravitational field at some point in space. As an example of scale, for applications in detecting oil and gas reserves, mineral deposits and subterranean structures, a sensitivity of tens of microgals per hertz$^{1/2}$ (μGal Hz$^{-1/2}$) are required.

To get an understanding of scale, 1 Gal = 1 cm s^{-2} = 0.01 m s^{-2}, roughly four orders of magnitude less than acceleration due to gravity experienced by a mass at the Earth's surface. A μGal is therefore ten orders of magnitude less than this. The gravity gradient (variation with height) above Earth's surface is about 3.1 microgals per centimetre of height (3.1 x 10^{-6} s^{-2}) and 1 Gal Hz$^{-1/2}$ is a measurement of 1 Gal over an integration time of 1 second, the variance of the acceleration from a value.

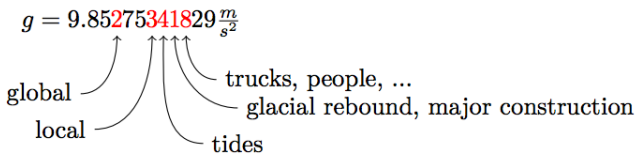


Figure M.1: An indication of the precision required to detect the acceleration due to gravity relative to that of the planet. Taken from [266].

As the density of structures around the gravimeter change, the gravitational field will change and this change can be measured to reveal some information about the structure.

Absolute gravity sensors measure the gravitational acceleration as a singular quantity. Currently, these devices are bulky, expensive and precise. A commercially available device like the Micro-g Lacoste FG5 has a mass of around 150 kg, costs $\$100,000$ and a sensitivity of 1.6 μGal Hz$^{-1/2}$ [267]. Relative gravity sensors measure some change in the gravitational field, for example how a spring will change length as the magnitude or direction of the gravitational field changes. These devices tend to be smaller and cheaper, but suffer from decreased accuracy and are naturally sensitive to changes in the environment. A Scintrex CG5 relative gravimeter still costs over $\$100,000$, has a precision of 2 μGal Hz$^{-1/2}$, is only 8 kg but is susceptible to drift, that is, the change in time of the measured data in unpredictable ways [268].

Gravity sensing applications are centred around the ability to detect density of masses that cannot be seen directly. In some ways, gravity sensors can be thought of as X-Ray vision - they see through barriers to gain information of what might be on the other side. To this end, the applications include

natural resource detection, tidal measurments, magma flows, climate science, detection of sinkholes and construction.

With higher sensitivity one can imagine that gravity sensors could be used to detect tiny changes in gravitational fields induced by objects with significantly less mass than, say, a planet. This might include detecting objects behind walls (pipes, structural deformities), tumours in cancer patients (non-intrusive procedures) or changing weather patterns (accumulation of rain).

As technology advances the expectations on progress are high. Gravity sensors are expected to become more precise and cheaper. Ideally, a device would be extremely sensitive, cheaper, small, lightweight, stable and accurate. In this case, a device could be deployed by a single user, a drone, in noisy environments, for applications in density measurements in systems as small as the human body.

As another example of scale, there is a difference in the acceleration experienced at the equator and at the poles. The Earth is not a perfect sphere; the radius to the equator is slightly larger than to the poles. In combination with the difference in the speed of rotation at these points the difference in the gravity is around 0.00005 Gal, or, 9.832 at the poles and 9.780 $\mathrm{m\,s^{-2}}$ at the equator [269].

Object	Mass/kg	Distance/m	Gravity/μGal	Gradient/ μGal $\mathrm{m^{-1}}$	Angle/ degree	Gravity change/ μGal
Earth	6.0×10^{24}	6.4×10^{6}	9.8×10^{8}	308	0	9.8×10^{8}
Optical table	1000	1.5	3.0	4	0	3.0
Aluminium spacers	1	0.1	0.7	13	0	0.7
Experimental physicist (A. P.)	90	1.0	0.7	1.2	45	0.5
Loaded truck	40 000	10	2.7	0.5	45	2.0
Physics lecture hall (demolished)	2.0×10^{6}	50	5.0	0.2	90	0.0
Hole (excavated)	2.0×10^{7}	100	13.3	0.3	85	1.3

Figure M.2: Absolute examples of the acceleration of various objects. Figure taken from [270].

M.1 Classical

Current classical devices include free-fall gravimeters, spring-based systems, superconducting gravimeters and MEMS.

M.1.1 Spring

One example of a classical gravity sensor that is on the cutting edge of research is a silicon based device that recognises slight changes in the Earth's gravitational field by measuring the varying position of a MEMS device integrated in silicon with light. MEMS devices have been used in phones as accelerometers for a long time now, but have never made the transition to gravimeters. Now, with increased precision and accuracy these devices have a sensitivity of 40 $\mu\mathrm{Gal\,Hz^{-1/2}}$ [271]; that is, changes corresponding to a change in height from the Earth's surface of around 600 metres can be distinguished from noise or a change in mass at an equal distance of 2×10^{17} kg (roughly 10^{-6}% of the mass of the earth).

The system consists of a set of cantilevers and a proof mass, operating under the same principle as spring mass systems in that the extension of the spring is dependent on the gravity at any point in time.

M.1.2 Superconducting

Also known as the ideal-spring gravimeter, superconducting gravimeters replace the spring with an ultralow temperature superconducting sphere held in place by an induced magnetic field. The sphere is responsive to minute variations in gravity. This type of gravimeter can achieve sensitivities of 1 nGal, one thousandth of one billionth (10^{-12}) of the Earth surface gravity.

M.1.3 Free-fall

The motion of a free falling corner-cube retroreflector in vacuum is monitored by a laser interferometer, see figure M.3, which detects optical interference to determine the rate of acceleration of gravity. Corner-cube absolute free-fall gravimeters are one of the most accurate types; however, their mechanical structure for repeated free falling is not suitable for mobile use and restricts their cycle time.

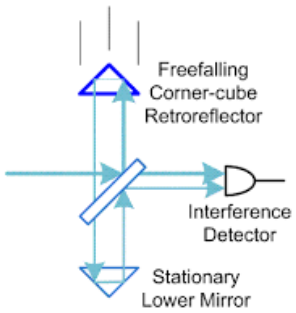


Figure M.3: Image taken from [272].

M.2 Quantum

As we have seen, there are different paradigms of gravimeters, which are limited to certain applications based on the shortcomings of the design in question. Atomic gravimeters may overcome many of these difficulties by providing precise measurements, over a long period of time in a stand-alone mobile instrument.

In principle they are similar to free-fall gravimeters. Like an optical interferometer, atomic interferometers measure the difference in phase of two atomic waves along two paths, putting the quantum in quantum gravity sensing.

Essentially, the process involves cooling atoms to millionths of a degree above zero. These matter waves then coherently split (dependent on the magnitude of the gravity) and recombine to produce interference fringes, see figure M.4. Light pulses act as beamsplitters and mirrors for the matter waves. The difference in height of the states manifests in the interferometry picture as a difference in phase between states. By measuring the relative populations it is possible to measure this phase and therefore calculate the height.

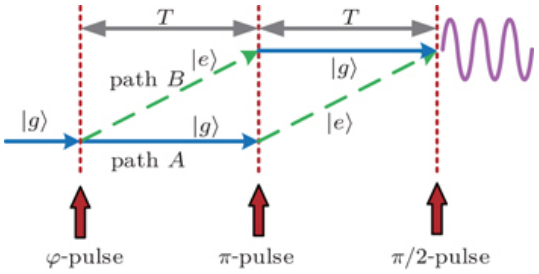


Figure M.4: Time period T between pulses, where $|g\rangle$ and $|e\rangle$ represent the two occupied states of the system. Image taken from [273].

The process of atomic interferometry is more precisely described below and is described in more detail by Hauth et. al. [274].

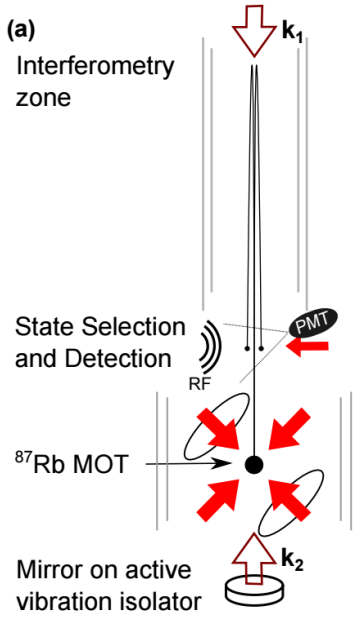


Figure M.5: k_1 and k_2 are the wavevectors of Rabi pulses. Image taken from [275].

In the first stage, which will be referred to as the preparation stage, rubidium-87 (Rb-87) atoms are loaded into a magneto-optical trap and laser cooled to a few μK. The cloud is launched upwards using far-detuned optical molasses (a 3D arrangement of lasers). The cloud of atoms is pumped to the $F = 2$ hyperfine ground state by the Raman process, a two-photon process where an atom is excited to a virtual energy level by off-resonant light and then de-excited to the next hyperfine

energy level, and atoms in a narrow velocity subclass are selected by applying a Raman pulse with a temporal Gaussian shape [276]. Atoms in a magnetically insensitive substate ($m_F = 0$) are selected with a microwave pulse. All other states and velocity classes are removed with resonant 'blow-away' laser pulses. The cloud is now at the top of the pipe.

In the second stage, which here will be called the interference phase, the atoms are fed through a conceptual Mach-Zehnder interferometer. A π-pulse in this analogy acts as a mirror and a $\pi/2$-pulse as a beamsplitter (see figure M.4). A $\pi/2$-pulse creates a superposition of the $F = 1$ and $F = 2$ states, which evolve along different paths due to photon recoil. A π-pulse inverts the states and finally they are combined by the last $\pi/2$-pulse.

In the measurement phase, back at the base of the interferometer, the relative populations of the states are compared by measuring the upper and lower state populations with a fluorescence detection system.

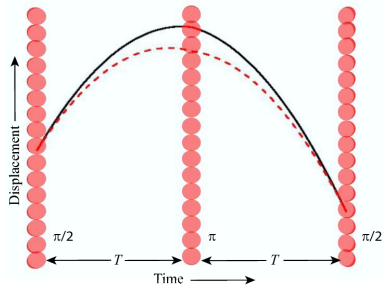


Figure M.6: Path divergence in atomic interferometry diagram. Image taken from [277].

Relative population of the upper state depends on the phase difference $\Delta\phi$ between paths of the interferometer:

$$P_{F_2} = \bar{P} + \frac{C}{2}\cos\Delta\phi, \tag{11}$$

where C is the contrast and $\bar{P}$ is the mean population. $\Delta\phi$ contains contributions due to the local acceleration of the atoms g and is given by a first approximation

$$\Delta\phi = (k_{\text{eff}}g = \alpha).T^2 + \Delta\phi_L, \tag{12}$$

where k_{eff} is the effective wavevector of the two Raman beams, $k_{\text{eff}} = |k_1 - k_2| \approx 2k$, T is the time spacing between the two pulses and $\Delta\phi_L$ the relative phase offset of the last interferometer pulse and it configurable so as to scan the interference fringe. α is a continuous radio frequency chirp applied to one of the Raman lasers such that the time varying Doppler shift of the atoms due to their velocity is approximately cancelled. Local acceleration can then be determined by adjusting α and $\Delta\phi_L$ until the phase difference is zero and hence the population of the $F = 2$ state is maximal.

M.2.1 Very Long Baseline Atom Interferometry and Atom Chip Interferometry

Another example of atomic interferometry applied in the field of gravity sensing is a proposed experimental scheme of very long baseline atom interferometry for application to fundamental sciences and measuring the Eötvös ratio at the order of 1×10^{-12} [278], which will impose new limits on the violation scenarios of the universality of free-fall.

Furthermore, Bose Einstein Condensates (BECs) promise to increase the accuracy of quantum gravity sensing below the μGal limit [279, 280]. An atom chip is a device that can trap and manipulate individual atoms just above its surface with a combination of optics and magnetic fields in vacuum. Using these chips applied to free falling BECs, observing free-fall over a distance as little as a few millimetres, shows promise to extend the accuracy of robust and compact gravimeters sensitive to variations of a few μGal and accurate to sub-μGal levels in an optimised setup.

M.3 Discussion

The greatest advantage of Quantum Gravity Sensors (QGSs) could end up being the cost of implementation. Reduced cost could open up the way for widespread adoption. Relatively few absolute gravimeters exist worldwide, because of the cost, and a globally distributed network could have implications for navigation, defence and climate science amongst other fields.

The Global Positioning System (GPS) (also called NavStar) is how our phones tell us where we are in the world. Signals from four satellites are coordinated to calculate our position based on the travel time of the signals from the satellites and the position of the satellites at that moment in time. Without the fourth ('time-keeping') satellite, your phone might only know your position approximately, for example, if you are in a city and it can only connect with three satellites. The approximation comes in when the GPS assumes you are at sea level.

Currently, very precise absolute gravimeters are expensive. Quantum devices based on atomic interferometry may fulfil the requirements of a globally distributed network and have even been demonstrated to work on-chip, these devices may one day be mobile, sensitive and resistant to drift. A network of these devices might be used to better define the shape of the Earth, calibrate other gravity instruments, determine the height of landmasses and, using the same principle as accelerometers, better inform and work alongside GPS systems for tracking and positioning in urban environments [281].

Further, data on the accumulation of water vapour locally could be fed into global climate models and allow for better prediction of weather patterns. A cheap distributed network might act as a warning system for natural disasters such as earthquakes and volcanoes by tracking the movements of vertical shifts of tectonic plates and changing magma flows beneath the surface.

A globally distributed network of sensitive, mobile and precise gravimeters will feed in a lot of information into climate science, including to better define the shape of the Earth and track the movement of water and precipitation around the world. Through the NASA GRACE experiment,

satellite measurements of the effect of water build-up on gravity measurements has already demonstrated the application of this. Quantum devices based on atomic interferometry may fulfil these requirements and have even been demonstrated to work on-chip.

With more data, the models we use to predict the weather and climate change will be better equipped to deal with climate change and humanity's impact on the world. Also, gravity sensors can be used to track magma flows and tectonic plate movements, which may give us better predictive tools for natural disasters.

On a local level, cheaper gravity sensing would have applications in massive infrastructure projects, road maintenance and construction. Taking this idea further it may be possible one day to detect tiny variations behind walls (pipes, foundations).

Classical gravity sensors tend to be bulky, expensive and susceptible to drift. QGSs aim to be mobile, sensitive and cheaper than their classical counterparts and may one day even be precise enough to detect pipes, load bearing walls and structural issues in our own homes.

In the field of construction, gravity sensors can be used in big infrastructure projects to detect sinkholes and see underground when planning building projects. Gravity sensors detect variations in mass by the gravity experienced as a result of that mass. QGSs could one day be so precise, and cost so little, as to be used to see through walls in our own homes.

N Faster Recommender Systems

With over one billion websites on the World Wide Web [282], we need something other than search engines to find a new band to hear, a highly rated movie to watch or news articles about a specific topic. User interfaces that help us to find information, products and services that are in accordance with our interests have become almost a requirement for any serious website. One of the tools to achieve this is the inclusion of a recommender system.

Some websites present users with personalised information by letting them choose from a set of predefined topics of interest. Users, however, do not always know what they are specifically interested in beforehand and their interests may change overtime which would require them to change their selection frequently. Recommender systems provide personalised information by analysing the user's interests from traces of interaction with that user. These systems have changed the way websites communicate with their users becoming a standard element on a modern web presence.

N.1 Classical

Recommender systems sort through massive amounts of data to identify potential user preferences [283]. Most recommendation systems take one of the two following basic approaches.

N.1.1 Content-Based Filtering

Content-based recommender systems try to find items similar to those a given user has liked or used in the past. In a content-based system, a profile which is a record of important characteristics of each item has to be created. In simple cases, these properties can be the genre of a movie, the musicians in a band, the language or author of a book, the brand of a product, etc. For more complicated items like document collections and images, the property assignment can be a more challenging task. Making the users tag the documents, images and even full websites has been one of the approaches to ease this challenge.

In this approach, not only item profiles need to be created. We need to create user profiles with the same components as the item ones that describe the user's preferences and a comparison can be performed. From the profiles, vectors in a particular space are defined, and from these, we can estimate the degree to which a user would prefer an item by computing a certain arbitrarily defined distance function between the user's and item's vectors. Those elements that minimise this function are the ones that are recommended to the user.

It is worth mentioning that a different approach using these item profiles can be used when the problem is treated as a machine learning problem [284].

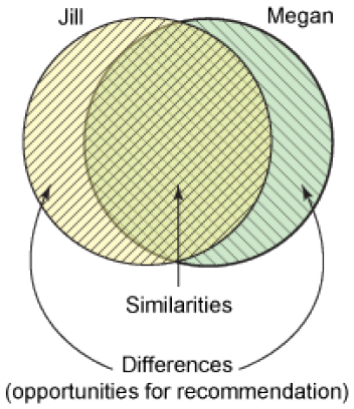


Figure N.1: Collaborative filtering is one of the common approaches to create recommender systems. The basic idea behind it is that it gives recommendations based on the few differences of very similar users. Image taken from [283].

N.1.2 Collaborative filtering

In collaborative filtering, the system generates recommendations using explicit or implicit preferences from many users ignoring the item's representation. These systems recommend items based on similarity measures between users. The items recommended to a user are those preferred by similar users. As depicted in figure N.1, the basic idea of collaborative filtering is to find two similar users but then extract the differing elements to create the recommendations. We can notice that this approach avoids the need of creating item profiles, but in exchange, the measure of similarity should be built carefully since a good algorithm should find the sweet spot where two users are not too similar for the space of recommendations be very narrow, but close enough that users have similiar interests with high probability.

The streaming media company Netflix, Inc. uses this kind of recommender system in their online service. In fact, they offered a prize of one million dollars for the first algorithm that could beat its own recommendation system by 10% [285].

N.2 Quantum

Even when these and even more complex versions of recommender systems have been tested for many years, we can see that all these algorithms deal with the problem of finding similar items or users to given ones in a big search space. Even when state-of-the-art recommender systems use complex algorithms to improve their accuracy and efficiency, in the end, one can think of them as similarity searching procedures. This year Chakrabarty et. al. have proposed a quantum algorithm suitable to be implemented within a recommender system. They use a dynamic Grover's search algorithm to define the goals for a recommendation system based on binomial similarity giving quadratic speedup over traditional classical unstructured recommender systems [286].

Grover's search algorithm is one of the most clear examples of how quantum algorithms provide

a fundamental advantage in terms of resources when compared with the classical ones. Grover's algorithm finds (in an unstructured way) with high probability the unique input to an oracle function that produces a particular output value, using just on the order of $\sqrt{N}$ evaluations of the function, where N is the size of the search space [287]. The difference between the standard Grover's algorithm and its dynamic version is that, instead of using a static oracle function f, a dynamic selection function f_s that selects a given state x with certain probability $P_s(x)$ is used:

$$f_s = \begin{cases} 1 & \text{if } |x\rangle \text{ is selected with } P_s(x) \\ 0 & \text{otherwise.} \end{cases} \tag{13}$$

The recommendation problem can be stated as follows. Given an unstructured search space S with a total number of elements (states) $N = 2^n$, we need to find M recommended states for a given search result $|x\rangle$. Let the similarity function $S(x, y)$ of two pure states $|x\rangle$, $|y\rangle$ represent a measure of the likeliness of these two states to be recommended for each other.

The probability function $P_s(x)$ can be built for the selection function f_s to be effective in a dynamic system. Actually, if the similarity function is given by the Hamming distance between the states [288], the probability of selection is given by

$$e^{-log(\sqrt[n]{K}-1)S(x,y)}. \tag{14}$$

Then, the states which are very similar to the searched state would have a higher selection probability and with this the Grover's search algorithm gives the usual quadratic speedup in the search of recommendations.

N.3 Discussion

This is one of the clear examples of how quantum computers are going to affect our lives even when the physical processor might not be in our houses. For instance, a quantum processor connected to the servers of the website is going to run this kind of algorithm. Then, classical computers are going to post-process the outcomes and finally give us the results for recommendations.

It is worth mentioning that another approach to develop quantum enhanced recommender systems could be QML. As it was mentioned before, machine learning has been used for content-based recommender algorithms and then, QML might give a boost in the power of these algorithms.

O Video Games

Video games are one of the main sources of entertainment nowadays. From its origin with the famous game "Pong", video games spread into people's houses in the form of consoles and are now present even in their smartphones. As of 2015, video games generated sales of $74 billion USD annually worldwide, and were the third largest segment in the U.S. entertainment market, behind broadcast and cable TV. It is then natural to ask oneself if quantum technologies will have an impact on the video game industry and help it develop and improve games.

O.1 Classical

A classical video game console nowadays heavily depends on a GPU. A GPU is a specialised electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device. Their highly parallel structure makes them more efficient than general-purpose CPUs for algorithms where the processing of large blocks of data is done in parallel. The classical video game improvement is then closely linked to the advent of ever increasingly powerful GPUs.

O.1.1 The Graphics Processing Unit

A processing graphics card is a printed circuit board that houses a processor and Random Access Memory (RAM). It also has an input/output system (BIOS) chip, which stores the card's settings and performs diagnostics on the memory, input and output at startup. As mentioned before, a GPU is designed specifically for performing the complex mathematical and geometric calculations necessary for graphics rendering. To improve image quality, the processors use:

- Full scene anti aliasing, which smoothes the edges of 3D objects;
- Anisotropic filtering, which makes images look crisper.

Some of the fastest GPUs have more transistors than the average CPU. A GPU produces a lot of heat, so it is usually located under a heat sink or a fan. In addition to its processing power, a GPU uses special programming to help it analyse and use data.

As the GPU creates images, it needs somewhere to hold information and completed pictures. It uses the card's RAM for this purpose, storing data about each pixel, its colour and its location on the screen. Part of the RAM can also act as a frame buffer, meaning that it holds completed images until it is time to display them. Typically, video RAM operates at very high speeds and is dual ported, meaning that the system can read from it and write to it at the same time. The RAM connects directly to the Digital-to-Analog Converter (DAC). This converter, called the RAMDAC, translates the image into an analog signal that the monitor can use. Some cards have multiple RAMDAC, which can improve performance and support more than one monitor.

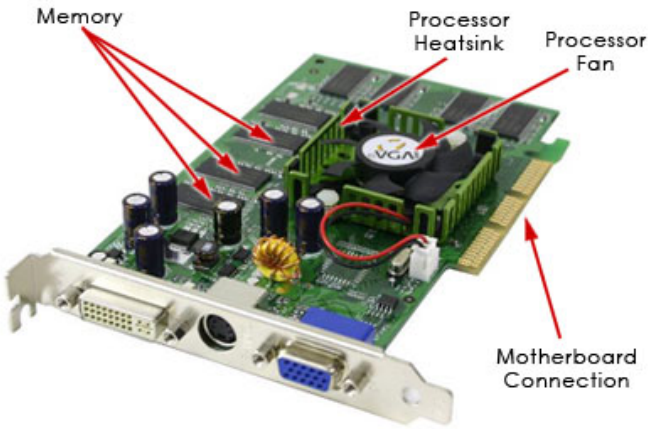


Figure O.1: A sketch of a GPU with some of its components. Image taken from [289].

A good overall measurement of a card's performance is its frame rate, measured in frames per second (fps). The frame rate describes how many complete images the card can display per second. The human eye can process about 25 frames every second, but fast-action games require a frame rate of at least 60 fps to provide smooth animation and scrolling. Components of the frame rate are:

- Triangles or vertices per second: 3D images are made of triangles or polygons. This measurement describes how quickly the GPU can calculate the whole polygon or the vertices that define it. In general, it describes how quickly the card builds a wire frame image.
- Pixel fill rate: This measurement describes how many pixels the GPU can process in a second, which translates to how quickly it can rasterise the image.

O.2 Quantum

How can quantum technologies improve the performance of video games? Which features or components of a video game will be improved? In this section, we shall explore two possible approaches to answer these questions. The first one will be an algorithm approach. We will discuss the possibility of a video game being based on quantum algorithms. The second approach will be a hardware approach. We shall consider whether there is a physical component used for performing the game which can be improved with quantum technologies. This improvement would not be done directly to the game itself, but to its outputs.

O.2.1 The Algorithm Approach

One way forward would be creating specific algorithms for the games themselves. Is there a way to perform the code in a quantum manner? Although not impossible, this scenario is improbable. A

single game is built on multiple lines of code and algorithms, and it is a dynamical system which responds to the player's actions. Since quantum algorithms are designed for very specific tasks, a single or few quantum algorithms would not be able to reproduce the game in its entirety. Only particular assignments would be done with quantum algorithms, e.g. perform a search of some key or introduce randomness on a given instance of the game. But even in this case, we have to ask some questions.

Firstly, does the performed task fall into the cases where the quantum algorithm executes faster than the classical counterpart? In other words, even though the used quantum algorithm has a better complexity class, it does not mean that it will perform faster than its classical counterpart in all instances. As an example, the Shor's algorithm for factoring primes only executes faster than the general number field sieve for numbers with more than 512 bits. It might be the case that the problem to be solved within the game is still in the range where the classical algorithm is better than the quantum one.

Secondly, even if a given task within the game can be substantially improved with a quantum algorithm, will the whole program, or the whole game, benefit from a substantial speedup? This is not necessarily true as depicted by the Amdahl's law [290]. This is a formula that gives the theoretical speedup in latency of the execution of a task at fixed workload that can be expected of a system whose resources are improved. It is often used in parallel computing to predict the theoretical speedup when using multiple processors. Amdahl's argument assumes that the system can be split up into a part that benefits from the improvement of the resources of the system, and another that does not. In our example of the video games, even if the part that benefits from the improvement has a speedup of, for example, 10 times, because it is such a small part of the whole program, and we saw above that it would probably be the case, the overall speedup might be less than 1% (see figure O.2). The classical part of the game will greatly limit the quantum speedup.

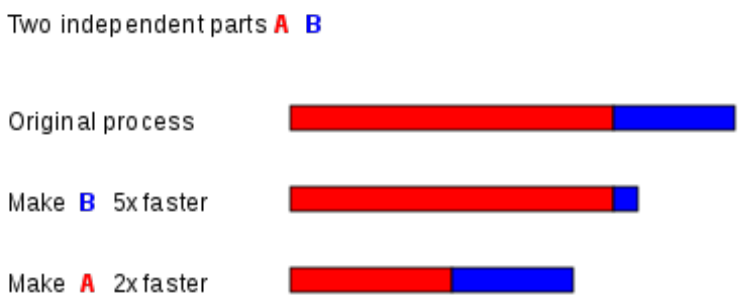


Figure O.2: Assume that a task has two independent parts, A and B. Part B takes roughly 25% of the time of the whole computation. By working very hard, one may be able to make this part 5 times faster, but this reduces the time of the whole computation only slightly. In contrast, one may need to perform less work to make part A perform twice as fast. This will make the computation much faster than by optimizing part B, even though part B's speedup is greater in terms of the ratio, (5 times versus 2 times). Image taken from [291].

Thirdly, these tasks will require a quantum computer to run. Having a quantum computer just to

perform some quantum algorithms for the speedup of some small part of the game seems unnecessary. This is because the overall impact would be negligible, as we just saw. We should aim at a general and important task that could be greatly improved by quantum technology. This leads us to the next approach.

O.2.2 The Hardware Approach

Another approach would be an output or hardware approach. As mentioned in the previous section, the speed heavily depends on a GPU. Their highly parallel structure makes them more efficient than general-purpose CPUs for algorithms where the processing of large blocks of data is done in parallel. The GPU seems the perfect part of a video game console to try to improve using quantum technologies, since its parallelism is exactly the feature that a quantum computer is based on. Therefore, the video game itself would be written and performed classically, while the graphics and the image processing would be executed by a quantum GPU.

A quantum GPU would be a quantum system solely focused on image processing. Even though a very recent field, quantum image processing already has interesting quantum algorithms for particular problems and also proposals for quantum image representation, e.g. qubit lattice [292, 293], real ket [294] and flexible representation of quantum images [295]. As an example, one of the ideas to represent a quantum image is to use a quantum register prepared in the state $|I\rangle = |C\rangle\,|P\rangle$, where C is an m-qubit register. This quantum state integrates both colour and position information. Pixel positions are coded in $|P\rangle$ using $2n$ qubits (it is possible to encode the information using qutrits, i.e. three level systems). The colour information of a single pixel is encoded using a single qubit [293, 295]:

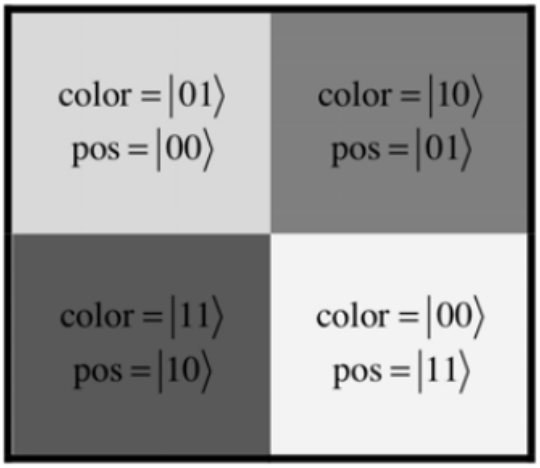
$$|\phi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\gamma}\sin\frac{\theta}{2}\,|1\rangle\,.$$

The real parameter θ encodes the frequency of the electromagnetic wave, while γ is left uninitialised. Therefore our total state is

$$|I\rangle = |C\rangle\,|P\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}\sum_{j=0}^{2^m-1}\alpha_{ij}\,|j\rangle\,|i\rangle\,.$$

Coefficients α_{ij}, with $\sum_{j=0}^{2^m-1}|\alpha_{ij}|^2 = 1$ for all i with $0 \leq i \leq 2^{2n}$, are used to express the colour of a pixel with position i by means of a superposition of all possible colours. For a given pixel i, coefficients α_{ij} take the value 1 if the colour of the pixel is j, and 0 otherwise. This is illustrated in figure O.3 with a simple example of a 2×2 image with four colours.

Even though this approach presents positive aspects, e.g. the visual information can be accurately retrieved using a statistical procedure involving multiple measurements of identically prepared states, it has some downsides, e.g. it is not suited for computing the histogram of an image,



$$|Q\rangle = \frac{1}{\sqrt{2^2}} \sum_{i=0}^{2^2-1} \sum_{j=0}^{2^2-1} \alpha_{ij} |j\rangle |i\rangle =$$

$$= \frac{1}{\sqrt{2^2}} (|01\rangle|00\rangle + |10\rangle|01\rangle + |11\rangle|10\rangle + |00\rangle|11\rangle)$$

$$\alpha_{00} = 0,\ \alpha_{01} = 1,\ \alpha_{02} = 0,\ \alpha_{03} = 0$$
$$\alpha_{10} = 0,\ \alpha_{11} = 0,\ \alpha_{12} = 1,\ \alpha_{13} = 0$$
$$\alpha_{20} = 0,\ \alpha_{21} = 0,\ \alpha_{22} = 0,\ \alpha_{23} = 1$$
$$\alpha_{30} = 1,\ \alpha_{31} = 0,\ \alpha_{32} = 0,\ \alpha_{33} = 0$$

Figure O.3: Example of a simple 2×2 quantum image with four possible colours (two qubits are used to represent the colour information and two qubits encode the position of each pixel. Image taken from [296].

which represents the relative frequency of occurrence of the various colours (grey levels) in the image.

O.3 Discussion

Regarding the quantum algorithms for particular problems related to image processing, a few quantum algorithms have been suggested for the rendering problem [297, 298] and computational geometry [299]. Even the important task of image segmentation found a quantum analogue based on quantum circuit schemes [296], and the classical RANdom SAmple Consensus voting scheme (RANSAC) algorithm, vital for fundamental matrix estimation, trifocal tensor estimation, camera pose estimation, and structure from motion and shape detection, was translated into a quantum version [300]. This translation was done by identify the RANSAC algorithm as a search algorithm, which in turn has the powerful Grover algorithm as a quantum counterpart. All these algorithms,

if performed by a quantum computer specifically designed for image processing and graphics complexity, just like a GPU, could greatly improve the quality and performance of a video game.

When we go down to the hardware problem itself, it always ends with the task of building a quantum computer, which by itself is an amazing challenge. It may be possible to develop a quantum system solely for graphics issues. Therefore, it could be possible to have quantum technologies impacting the video games industry before the advent of full quantum computer However, the algorithms aforementioned may require a universal quantum machine to carry out all the calculations. Nonetheless, quantum technologies will probably find applications in the video game industry, not in the development of games themselves, but in external, and highly parallelised, tasks such as image processing.

References

[1] Homeland Security Research. Quantum computing market & technologies - 2017-2024. *Homeland Security Research*, 2017.

[2] Central Compilation & Translation Press. The 13th five-year plan for economic and social development of the people's republic of china. *Central Compilation & Translation Press*, 2016.

[3] White House. America first: A budget blueprint to make america great again. *March*, 16:50, 2017.

[4] IARPA. Quantum programs at iarpa. https://www.iarpa.gov/index.php/research-programs/quantum-programs-at-iarpa, 2017.

[5] HM Treasury. Autumn statement 2013. *Crown copyright*, 2013.

[6] Qurope. Quantum manifesto: A new era of technology. *Qurope*, 2016.

[7] Freeke Heijman te Paske. Global developments in quantum technologies. https://connect.innovateuk.org/documents/11487824/26842605/Global+Developments+in+Quantum+Technology/, 2015.

[8] George Stoye. Uk health spending, 2017.

[9] Kaare Christensen, Gabriele Doblhammer, Roland Rau, and James W Vaupel. Ageing populations: the challenges ahead. *The lancet*, 374(9696):1196–1208, 2009.

[10] Joseph A DiMasi, Henry G Grabowski, and Ronald W Hansen. Innovation in the pharmaceutical industry: new estimates of r&d costs. *Journal of health economics*, 47:20–33, 2016.

[11] OECD. Fiscal sustainability of health systems: Bridging health and finance perspectives. *OECD*, 2015.

[12] Richard P Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6):467–488, 1982.

[13] Mary Meeker. Internet trends. kpcb.com/InternetTrends, 2017.

[14] Meredydd Williams, Louise Axon, Jason RC Nurse, and Sadie Creese. Future scenarios and challenges for security and privacy. In *Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), 2016 IEEE 2nd International Forum on*, pages 1–6. IEEE, 2016.

[15] Lee Rainie, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish. Anonymity, privacy, and security online. *Pew Research Center*, 5, 2013.

[16] World Economic Forum. Global risks 2017. http://reports.weforum.org/global-risks-2017/part-1-global-risks-2017/, 2017.

[17] Jeff Tollefson and Kenneth R Weiss. Nations adopt historic global climate accord: agreement commits world to holding warming'well below'2 [degrees] c. *Nature*, 582(7582):315–317, 2015.

[18] IHS Technology Sam Wilkinson. Grid-connected energy storage report, 2015.

[19] World Economic Forum. Renewable infrastructure investment handbook: A guide for institutional investors, 2016.

[20] Paul Korzeniowski. Digital entertainment in the home: Technologies and global markets. *bccresearch*, 2014.

[21] Yaoyao Clare Duan. *Market research of commercial recommendation engines for online and offline retail*. PhD thesis, Massachusetts Institute of Technology, 2014.

[22] Trabesinger. Quantum simulation. *Nature Phys*, 8:263–280, 2012.

[23] Masuo Suzuki. *Quantum Monte Carlo methods in condensed matter physics*. World scientific, 1993.

[24] Matthias Troyer and Uwe-Jens Wiese. Computational complexity and fundamental limitations to fermionic quantum monte carlo simulations. *Physical review letters*, 94(17):170201, 2005.

[25] Alexander L Fetter and John Dirk Walecka. *Quantum theory of many-particle systems*. Courier Corporation, 2012.

[26] Iulia Buluta and Franco Nori. Quantum simulators. *Science*, 326(5949):108–111, 2009.

[27] IM Georgescu, Sahel Ashhab, and Franco Nori. Quantum simulation. *Reviews of Modern Physics*, 86(1):153, 2014.

[28] S Somaroo, CH Tseng, TF Havel, Raymond Laflamme, and David G Cory. Quantum simulations on a quantum computer. *Physical review letters*, 82(26):5381, 1999.

[29] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[30] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. AAPT, 2002.

[31] Seth Lloyd et al. Universal quantum simulators. *SCIENCE-NEW YORK THEN WASHINGTON-*, pages 1073–1077, 1996.

[32] Jianwei Wang, Stefano Paesani, Raffaele Santagati, Sebastian Knauer, Antonio A Gentile, Nathan Wiebe, Maurangelo Petruzzella, Jeremy L O'Brien, John G Rarity, Anthony Laing, et al. Experimental quantum hamiltonian learning. *Nature Physics*, 2017.

[33] Fumiko Yamaguchi and Yoshihisa Yamamoto. Quantum simulation of the t–j model. *Superlattices and microstructures*, 32(4):343–345, 2002.

[34] Efstratios Manousakis. A quantum-dot array as model for copper-oxide superconductors: A dedicated quantum simulator for the many-fermion problem. *Journal of low temperature physics*, 126(5-6):1501–1513, 2002.

[35] AL Rakhmanov, VA Yampol'Skii, JA Fan, Federico Capasso, and Franco Nori. Layered superconductors as negative-refractive-index metamaterials. *Physical Review B*, 81(7):075101, 2010.

[36] Daniel A Lidar and Haobin Wang. Calculating the thermal rate constant with exponential speedup on a quantum computer. *Physical Review E*, 59(2):2429, 1999.

[37] Ivan Kassal, Stephen P Jordan, Peter J Love, Masoud Mohseni, and Alán Aspuru-Guzik. Polynomial-time quantum algorithm for the simulation of chemical dynamics. *Proceedings of the National Academy of Sciences*, 105(48):18681–18686, 2008.

[38] Benjamin P Lanyon, James D Whitfield, Geoff G Gillett, Michael E Goggin, Marcelo P Almeida, Ivan Kassal, Jacob D Biamonte, Masoud Mohseni, Ben J Powell, Marco Barbieri, et al. Towards quantum chemistry on a quantum computer. *Nature chemistry*, 2(2):106–111, 2010.

[39] Dawei Lu, Nanyang Xu, Ruixue Xu, Hongwei Chen, Jiangbin Gong, Xinhua Peng, and Jiangfeng Du. Simulation of chemical isomerization reaction dynamics on a nmr quantum simulator. *Physical review letters*, 107(2):020501, 2011.

[40] Ivan Kassal, James D Whitfield, Alejandro Perdomo-Ortiz, Man-Hong Yung, and Alán Aspuru-Guzik. Simulating chemistry using quantum computers. *Annual review of physical chemistry*, 62:185–207, 2011.

[41] A Perdomo-Ortiz, M Drew-Brook, N Dickson, G Rose, and A Aspuru-Guzik. Experimental realization of a 8-qubit quantum-adiabatic algorithm for a lattice protein model: Towards optimization on a quantum computer. *Manuscript in preparation*, 2010.

[42] William R Hendee and Christopher J Morgan. Magnetic resonance imaging part i—physical principles. *Western Journal of Medicine*, 141(4):491, 1984.

[43] Matti Hämäläinen, Riitta Hari, Risto J Ilmoniemi, Jukka Knuutila, and Olli V Lounasmaa. Magnetoencephalography—theory, instrumentation, and applications to noninvasive studies of the working human brain. *Reviews of modern Physics*, 65(2):413, 1993.

[44] David A Kaiser. Basic principles of quantitative eeg. *Journal of Adult Development*, 12(2-3):99–104, 2005.

[45] Vincent Beroulle, Yves Bertrand, Laurent Latorre, and Pascal Nouet. Monolithic piezoresistive cmos magnetic field sensors. *Sensors and Actuators A: Physical*, 103(1):23–32, 2003.

[46] Henry H Yang, NV Myung, Jeffrey Yee, D-Y Park, B-Y Yoo, Morton Schwartz, Ken Nobe, and Jack W Judy. Ferromagnetic micromechanical magnetometer. *Sensors and Actuators A: Physical*, 97:88–97, 2002.

[47] Pavel Ripka. Magnetic sensors for industrial and field applications. *Sensors and Actuators A: Physical*, 42(1-3):394–397, 1994.

[48] John Clarke, Wolfgang M Goubau, and Mark B Ketchen. Tunnel junction dc squid: fabrication, operation, and performance. *Journal of Low Temperature Physics*, 25(1):99–144, 1976.

[49] Claudia D Tesche and John Clarke. Dc squid: noise and optimization. *Journal of Low Temperature Physics*, 29(3):301–331, 1977.

[50] Ernst Niedermeyer and FH Lopes da Silva. *Electroencephalography: basic principles, clinical applications, and related fields*. Lippincott Williams & Wilkins, 2005.

[51] G Bison, R Wynands, and A Weis. A laser-pumped magnetometer for the mapping of human cardiomagnetic fields. *Applied Physics B*, 76(3):325–328, 2003.

[52] R Mhaskar, S Knappe, and J Kitching. A low-power, high-sensitivity micromachined optical magnetometer. *Applied Physics Letters*, 101(24):241105, 2012.

[53] G Bison, N Castagna, A Hofer, P Knowles, J-L Schenker, M Kasprzak, H Saudan, and A Weis. A room temperature 19-channel magnetic field mapping device for cardiac signals. *Applied Physics Letters*, 95(17):173701, 2009.

[54] Dmitry Budker and MV Romalis. Optical magnetometry. *arXiv preprint physics/0611246*, 2006.

[55] H Xia, A Ben-Amar Baranga, D Hoffman, and MV Romalis. Magnetoencephalography with an atomic magnetometer. *Applied Physics Letters*, 89(21):211104, 2006.

[56] Cort N Johnson, PDD Schwindt, and M Weisend. Multi-sensor magnetoencephalography with atomic magnetometers. *Physics in medicine and biology*, 58(17):6065, 2013.

[57] IM Savukov, VS Zotev, PL Volegov, MA Espy, AN Matlashov, JJ Gomez, and RH Kraus. Mri with an atomic magnetometer suitable for practical imaging applications. *Journal of Magnetic Resonance*, 199(2):188–191, 2009.

[58] HB Dang, AC Maloof, and MV Romalis. Ultrahigh sensitivity magnetic field and magnetization measurements with an atomic magnetometer. *Applied Physics Letters*, 97(15):151110, 2010.

[59] D Drung, C Abmann, J Beyer, A Kirste, M Peters, F Ruede, and Th Schurig. Highly sensitive and easy-to-use squid sensors. *IEEE Transactions on Applied Superconductivity*, 17(2):699–704, 2007.

[60] IK Kominis. Sub-shot-noise magnetometry with a correlated spin-relaxation dominated alkali-metal vapor. *Physical review letters*, 100(7):073002, 2008.

[61] M Koschorreck, M Napolitano, B Dubost, and MW Mitchell. Sub-projection-noise sensitivity in broadband atomic magnetometry. *Physical review letters*, 104(9):093602, 2010.

[62] V Shah, G Vasilakis, and MV Romalis. High bandwidth atomic magnetometery with continuous quantum nondemolition measurements. *Physical review letters*, 104(1):013601, 2010.

[63] RJ Sewell, M Koschorreck, M Napolitano, B Dubost, N Behbood, and MW Mitchell. Magnetic sensitivity beyond the projection noise limit by spin squeezing. *Physical review letters*, 109(25):253605, 2012.

[64] D Sheng, S Li, N Dural, and MV Romalis. Subfemtotesla scalar atomic magnetometry using multipass cells. *Physical review letters*, 110(16):160802, 2013.

[65] Travis Horrom, Robinjeet Singh, Jonathan P Dowling, and Eugeniy E Mikhailov. Quantum-enhanced magnetometer with low-frequency squeezing. *Physical Review A*, 86(2):023803, 2012.

[66] Florian Wolfgramm, Alessandro Cere, Federica A Beduini, Ana Predojević, Marco Koschorreck, and Morgan W Mitchell. Squeezed-light optical magnetometry. *Physical review letters*, 105(5):053601, 2010.

[67] Michael A Taylor and Warwick P Bowen. Quantum metrology and its application in biology. *Physics Reports*, 615:1–59, 2016.

[68] Marcus W Doherty, Neil B Manson, Paul Delaney, Fedor Jelezko, Jörg Wrachtrup, and Lloyd CL Hollenberg. The nitrogen-vacancy colour centre in diamond. *Physics Reports*, 528(1):1–45, 2013.

[69] Nir Bar-Gill, Linh M Pham, Andrejs Jarmola, Dmitry Budker, and Ronald L Walsworth. Solid-state electronic spin coherence time approaching one second. *arXiv preprint arXiv:1211.7094*, 2012.

[70] Gopalakrishnan Balasubramanian, Philipp Neumann, Daniel Twitchen, Matthew Markham, Roman Kolesov, Norikazu Mizuochi, Junichi Isoya, Jocelyn Achard, Johannes Beck, Julia Tissler, et al. Ultralong spin coherence time in isotopically engineered diamond. *Nature materials*, 8(5):383, 2009.

[71] CL Degen. Scanning magnetic field microscope with a diamond single-spin sensor. *Applied Physics Letters*, 92(24):243111, 2008.

[72] JR Maze, PL Stanwix, JS Hodges, S Hong, JM Taylor, P Cappellaro, L Jiang, MV Gurudev Dutt, E Togan, AS Zibrov, et al. Nanoscale magnetic sensing with an individual electronic spin in diamond. *Nature*, 455(7213):644, 2008.

[73] JM Taylor, P Cappellaro, L Childress, L Jiang, D Budker, PR Hemmer, A Yacoby, R Walsworth, and MD Lukin. High-sensitivity diamond magnetometer with nanoscale resolution. *arXiv preprint arXiv:0805.1367*, 2008.

[74] Michael Sean Grinolds, Sungkun Hong, Patrick Maletinsky, Lan Luan, Mikhail D Lukin, Ronald Lee Walsworth, and Amir Yacoby. Nanoscale magnetic imaging of a single electron spin under ambient conditions. *arXiv preprint arXiv:1209.0203*, 2012.

[75] Yuichiro Matsuzaki, Takaaki Shimo-Oka, Hirotaka Tanaka, Yasuhiro Tokura, Kouichi Semba, and Norikazu Mizuochi. Hybrid quantum magnetic-field sensor with an electron spin and a nuclear spin in diamond. *Physical Review A*, 94(5):052330, 2016.

[76] Sebastian Zaiser, Torsten Rendler, Ingmar Jakobi, Thomas Wolf, Sang-Yun Lee, Samuel Wagner, Ville Bergholm, Thomas Schulte-Herbrüggen, Philipp Neumann, and Jörg Wrachtrup. Enhancing quantum sensing sensitivity by a quantum memory. *Nature communications*, 7, 2016.

[77] Thomas Wolf, Philipp Neumann, Kazuo Nakamura, Hitoshi Sumiya, Takeshi Ohshima, Junichi Isoya, and Jörg Wrachtrup. Subpicotesla diamond magnetometry. *Physical Review X*, 5(4):041001, 2015.

[78] Kazuo Tanaka, Kazuyuki Matsunaga, and Hua O Wang. Electroencephalogram-based control of an electric wheelchair. *IEEE transactions on robotics*, 21(4):762–766, 2005.

[79] Inaki Iturrate, Javier Antelis, and Javier Minguez. Synchronous eeg brain-actuated wheelchair with automated navigation. In *Robotics and Automation, 2009. ICRA'09. IEEE International Conference on*, pages 2318–2325. IEEE, 2009.

[80] Brice Rebsamen, Etienne Burdet, Cuntai Guan, Haihong Zhang, Chee Leong Teo, Qiang Zeng, Christian Laugier, and Marcelo H Ang Jr. Controlling a wheelchair indoors using thought. *IEEE intelligent systems*, 22(2), 2007.

[81] Tian-Ming Fu, Guosong Hong, Tao Zhou, Thomas G Schuhmann, Robert D Viveros, and Charles M Lieber. Stable long-term chronic brain mapping at the single-neuron level. *Nature methods*, 13(10):875–882, 2016.

[82] Paul Nuyujukian, Jonathan C Kao, Stephen I Ryu, and Krishna V Shenoy. A nonhuman primate brain–computer typing interface. *Proceedings of the IEEE*, 105(1):66–72, 2017.

[83] F.J.E.K.C. Duarte. Two-laser therapy and diagnosis device, September 28 1988. EP Patent App. EP19,880,302,468.

[84] L. Goldman. *Dye Laser Principles*. Academic Press, Boston, 1990.

[85] I. Garcia-Moreno A. Costela and C. Gomez. *Tunable Laser Applications*. CRC Press, Boca Raton, 3rd edition, 2016.

[86] M. Fox. *Quantum Optics: An Introduction*. Oxford Master Series in Physics. OUP Oxford, 2006.

[87] Wikipedia. Camera. https://en.wikipedia.org/wiki/Camera, 2017.

[88] Y. Shih. Quantum imaging. *IEEE Journal of Selected Topics in Quantum Electronics*, 13(4):1016–1030, July 2007.

[89] Jianming Wen, Morton H Rubin, and Yanhua Shih. Spatial resolution enhancement in quantum imaging beyond the diffraction limit using entangled photon-number state. *arXiv preprint arXiv:0812.2032*, 2008.

[90] Xi-Lin Wang, Luo-Kan Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Yu-Ao Chen, Chao-Yang Lu, and Jian-Wei Pan. Experimental ten-photon entanglement. *Phys. Rev. Lett.*, 117:210502, Nov 2016.

[91] A. Valencia, G. Scarcelli, M. D'Angelo, and Y. Shih. Two-photon "ghost" imaging with thermal light. In *2005 Quantum Electronics and Laser Science Conference*, volume 1, pages 557–559 Vol. 1, May 2005.

[92] Yan-Hua Zhai, Xi-Hao Chen, Da Zhang, and Ling-An Wu. Two-photon interference with true thermal light. *Phys. Rev. A*, 72:043805, Oct 2005.

[93] Shota Yokoyama, Ryuji Ukai, Seiji C. Armstrong, Chanond Sornphiphatphong, Toshiyuki Kaji, Shigenari Suzuki, Jun-ichi Yoshikawa, Hidehiro Yonezawa, Nicolas C. Menicucci, and Akira Furusawa. Ultra-large-scale continuous-variable cluster states multiplexed in the time domain. *Nat Photon*, 7(12):982–986, Dec 2013. Letter.

[94] Jun ichi Yoshikawa, Shota Yokoyama, Toshiyuki Kaji, Chanond Sornphiphatphong, Yu Shiozawa, Kenzo Makino, and Akira Furusawa. Invited article: Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing. *APL Photonics*, 1(6):060801, 2016.

[95] Ulrik L Andersen, Tobias Gehring, Christoph Marquardt, and Gerd Leuchs. 30 years of squeezed light generation. *Physica Scripta*, 91(5):053001, 2016.

[96] B. P. J. Abbott *et al.* Observation of gravitational waves from a binary black hole merger. *Phys. Rev. Lett.*, 116:061102, Feb 2016.

[97] E. S. Polzik, J. Carri, and H. J. Kimble. Spectroscopy with squeezed light. *Phys. Rev. Lett.*, 68:3020–3023, May 1992.

[98] Ian D. Leroux, Monika H. Schleier-Smith, and Vladan Vuletić. Orientation-dependent entanglement lifetime in a squeezed atomic clock. *Phys. Rev. Lett.*, 104:250801, Jun 2010.

[99] Michael A. Taylor, Jiri Janousek, Vincent Daria, Joachim Knittel, Boris Hage, Hans-A. Bachor, and Warwick P. Bowen. Subdiffraction-limited quantum imaging within a living cell. *Phys. Rev. X*, 4:011017, Feb 2014.

[100] Mohan Sarovar, Akihito Ishizaki, Graham R. Fleming, and K. Birgitta Whaley. Quantum entanglement in photosynthetic light-harvesting complexes. *Nat Phys*, 6(6):462–467, Jun 2010.

[101] Warren R Sanborn, Claus Chr Heuck, Raja El Aouad, and Wulf B Storch. Fluorescence microscopy for disease diagnosis and environmental monitoring. *World Health Organization Regional Office for the Eastern Mediterranean, Cairo, Egypt*, 2005.

[102] Maria Strianese, Maria Staiano, Giuseppe Ruggiero, Tullio Labella, Claudio Pellecchia, and Sabato D'Auria. Fluorescence-based biosensors. *Spectroscopic Methods of Analysis: Methods and Protocols*, pages 193–216, 2012.

[103] Jean Livet, Tamily A Weissman, Hyuno Kang, Ryan W Draft, Ju Lu, Robyn A Bennis, Joshua R Sanes, and Jeff W Lichtman. Transgenic strategies for combinatorial expression of fluorescent proteins in the nervous system. *Nature*, 450(7166):56, 2007.

[104] Xingyong Wu, Hongjian Liu, Jianquan Liu, Kari N Haley, Joseph A Treadway, J Peter Larson, Nianfeng Ge, Frank Peale, and Marcel P Bruchez. Immunofluorescent labeling of cancer marker her2 and other cellular targets with semiconductor quantum dots. *Nature biotechnology*, 21(1):41, 2003.

[105] Warren CW Chan and Shuming Nie. Quantum dot bioconjugates for ultrasensitive nonisotopic detection. *Science*, 281(5385):2016–2018, 1998.

[106] Marcel Bruchez, Mario Moronne, Peter Gin, Shimon Weiss, and A Paul Alivisatos. Semiconductor nanocrystals as fluorescent biological labels. *science*, 281(5385):2013–2016, 1998.

[107] W Russ Algar, Kimihiro Susumu, James B Delehanty, and Igor L Medintz. Semiconductor quantum dots in bioanalysis: crossing the valley of death, 2011.

[108] K David Wegner and Niko Hildebrandt. Quantum dots: bright and versatile in vitro and in vivo fluorescence imaging biosensors. *Chemical Society Reviews*, 44(14):4792–4834, 2015.

[109] Alan R Lowe, Jake J Siegel, Petr Kalab, Merek Siu, Karsten Weis, and Jan T Liphardt. Selectivity mechanism of the nuclear pore complex characterized by single cargo tracking. *Nature*, 467(7315):600, 2010.

[110] Yan-Fei Kang, Yu-Hao Li, Yang-Wu Fang, Yang Xu, Xiao-Mi Wei, and Xue-Bo Yin. Carbon quantum dots for zebrafish fluorescence imaging. *Scientific reports*, 5:11835, 2015.

[111] Yongqiang Dong, Ruixue Wang, Hao Li, Jingwei Shao, Yuwu Chi, Xiaomei Lin, and Guonan Chen. Polyamine-functionalized carbon quantum dots for chemical sensing. *Carbon*, 50(8):2810–2815, 2012.

[112] Yongqiang Dong, Ruixue Wang, Geli Li, Congqiang Chen, Yuwu Chi, and Guonan Chen. Polyamine-functionalized carbon quantum dots as fluorescent probes for selective and sensitive detection of copper ions. *Analytical chemistry*, 84(14):6220–6224, 2012.

[113] William J Peveler, Alberto Roldan, Nathan Hollingsworth, Michael J Porter, and Ivan P Parkin. Multichannel detection and differentiation of explosives with a quantum dot array. *ACS nano*, 10(1):1139–1146, 2015.

[114] Janina Hanne, Henning J Falk, Frederik Görlitz, Patrick Hoyer, Johann Engelhardt, Steffen J Sahl, and Stefan W Hell. Sted nanoscopy with fluorescent quantum dots. *Nature communications*, 6, 2015.

[115] Michael J Rust, Mark Bates, and Xiaowei Zhuang. Sub-diffraction-limit imaging by stochastic optical reconstruction microscopy (storm). *Nature methods*, 3(10):793–795, 2006.

[116] Jianquan Xu, Kayvan F Tehrani, and Peter Kner. Multicolor 3d super-resolution imaging by quantum dot stochastic optical reconstruction microscopy. *Acs Nano*, 9(3):2917–2925, 2015.

[117] Thomas Dertinger, Ryan Colyer, Gopal Iyer, Shimon Weiss, and Jörg Enderlein. Fast, background-free, 3d super-resolution optical fluctuation imaging (sofi). *Proceedings of the National Academy of Sciences*, 106(52):22287–22292, 2009.

[118] Yong Wang, Gilbert Fruhwirth, En Cai, Tony Ng, and Paul R Selvin. 3d super-resolution imaging with blinking quantum dots. *Nano letters*, 13(11):5233–5241, 2013.

[119] Zhao Yue, Fred Lisdat, Wolfgang J Parak, Stephen G Hickey, Liping Tu, Nadeem Sabir, Dirk Dorfs, and Nadja C Bigall. Quantum-dot-based photoelectrochemical sensors for chemical and biological detection. *ACS applied materials & interfaces*, 5(8):2800–2814, 2013.

[120] J Tanne, D Schafer, W Khalid, WJ Parak, and F Lisdat. Light-controlled bioelectrochemical sensor based on cdse/zns quantum dots. *Analytical chemistry*, 83(20):7778–7785, 2011.

[121] Itamar Willner, Fernando Patolsky, and Julian Wasserman. Photoelectrochemistry with controlled dna-cross-linked cds nanoparticle arrays. *Angewandte Chemie International Edition*, 40(10):1861–1864, 2001.

[122] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[123] Arash Habibi Lashkari, Mir Mohammad Seyed Danesh, and Behrang Samadi. A survey on wireless security protocols (wep, wpa and wpa2/802.11 i). In *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, pages 48–52. IEEE, 2009.

[124] IEEE. IEEE 802 Specifications.

[125] THe Free Dictionary. Network router.

[126] S Weinstein and Paul Ebert. Data transmission by frequency-division multiplexing using the discrete fourier transform. *IEEE transactions on Communication Technology*, 19(5):628–634, 1971.

[127] Ivan B Djordjevic and Bane Vasic. Orthogonal frequency division multiplexing for high-speed optical transmission. *Optics Express*, 14(9):3767–3775, 2006.

[128] Ye Geoffrey Li and Gordon L Stuber. *Orthogonal frequency division multiplexing for wireless communications*. Springer Science & Business Media, 2006.

[129] ISO. ISO/IEC FDIS 11801.

[130] Charles H Bennett and Stephen J Wiesner. Communication via one-and two-particle operators on einstein-podolsky-rosen states. *Physical review letters*, 69(20):2881, 1992.

[131] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[132] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.

[133] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

[134] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, 7(5):382–386, 2013.

[135] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, Jan 2007.

[136] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *arXiv preprint arXiv:1707.00542*, 2017.

[137] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[138] Mehdi Namazi, Giuseppe Vallone, Bertus Jordaan, Connor Goham, Reihaneh Shahrokhshahi, Paolo Villoresi, and Eden Figueroa. Free space quantum communication with quantum memory. In *Frontiers in Optics*, pages FF2C–3. Optical Society of America, 2016.

[139] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, et al. Ground-to-satellite quantum teleportation. *arXiv preprint arXiv:1707.00934*, 2017.

[140] Josephine Dias and Timothy C Ralph. Quantum repeaters using continuous-variable teleportation. *Physical Review A*, 95(2):022312, 2017.

[141] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. All-photonic quantum repeaters. *Nature communications*, 6, 2015.

[142] IDQuantique. *Clavis 2 Datasheet*.

[143] IDQuantique. *Clavis 3 Datasheet*.

[144] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.

[145] Cyril Branciard, Nicolas Gisin, Barbara Kraus, and Valerio Scarani. Security of two quantum cryptography protocols using the same four qubit states. *Physical Review A*, 72(3):032301, 2005.

[146] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, et al. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Physical Review X*, 6(1):011024, 2016.

[147] Damien Stucki, Claudio Barreiro, Sylvain Fasel, Jean-Daniel Gautier, Olivier Gay, Nicolas Gisin, Rob Thew, Yann Thoma, Patrick Trinkler, Fabien Vannel, and Hugo Zbinden. Continuous high speed coherent one-way quantum key distribution. *Opt. Express*, 17(16):13326–13334, Aug 2009.

[148] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, Feb 2004.

[149] Sima Bahrani, Mohsen Razavi, and Jawad A Salehi. Orthogonal frequency-division multiplexed quantum key distribution. *Journal of Lightwave Technology*, 33(23):4687–4698, 2015.

[150] EMVCo. Emv specifications.

[151] Steven J Murdoch, Saar Drimer, Ross Anderson, and Mike Bond. Chip and pin is broken. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 433–446. IEEE, 2010.

[152] Mike Bond, Omar Choudary, Steven J Murdoch, Sergei Skorobogatov, and Ross Anderson. Chip and skim: cloning emv cards with the pre-play attack. In *Security and Privacy (SP), 2014 IEEE Symposium on*, pages 49–64. IEEE, 2014.

[153] Jon Erickson. *Hacking: the art of exploitation*. No Starch Press, 2008.

[154] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017.

[155] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Cryptanalytic attacks on pseudorandom number generators. In *Fast Software Encryption*, pages 168–188. Springer, 1998.

[156] Saar Drimer, Steven J Murdoch, and Ross J Anderson. Optimised to fail: Card readers for online banking. In *Financial Cryptography*, volume 5628, pages 184–200. Springer, 2009.

[157] JL Duligall, MS Godfrey, KA Harrison, WJ Munro, and JG Rarity. Low cost and compact quantum key distribution. *New Journal of Physics*, 8(10):249, 2006.

[158] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, 7(5):382–386, 2013.

[159] Mohammad H Amin, Evgeny Andriyash, Jason Rolfe, Bohdan Kulchytskyy, and Roger Melko. Quantum boltzmann machine. *arXiv preprint arXiv:1601.02036*, 2016.

[160] Christine Vu. Research alliance builds new transistor for 5nm technology, June 2017.

[161] Michael A Nielsen. Cluster-state quantum computation. *Reports on Mathematical Physics*, 57(1):147–161, 2006.

[162] Daniel Gottesman and Isaac L Chuang. Quantum teleportation is a universal computational primitive. *arXiv preprint quant-ph/9908010*, 1999.

[163] Tadashi Kadowaki and Hidetoshi Nishimori. Quantum annealing in the transverse ising model. *Physical Review E*, 58(5):5355, 1998.

[164] Mark W Johnson, Mohammad HS Amin, Suzanne Gildert, Trevor Lanting, Firas Hamze, Neil Dickson, R Harris, Andrew J Berkley, Jan Johansson, Paul Bunyk, et al. Quantum annealing with manufactured spins. *Nature*, 473(7346):194, 2011.

[165] Vasil S Denchev, Sergio Boixo, Sergei V Isakov, Nan Ding, Ryan Babbush, Vadim Smelyanskiy, John Martinis, and Hartmut Neven. What is the computational value of finite-range tunneling? *Physical Review X*, 6(3):031015, 2016.

[166] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[167] Ashley Montanaro. Quantum algorithms: an overview. *NPJ Quantum Information*, 2:15023, 2016.

[168] Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, John M Martinis, and Hartmut Neven. Characterizing quantum supremacy in near-term devices. *arXiv preprint arXiv:1608.00263*, 2016.

[169] Masoud Mohseni, Peter Read, Hartmut Neven, Sergio Boixo, Vasil Denchev, Ryan Babbush, Austin Fowler, Vadim Smelyanskiy, John Martinis, et al. Commercialize early quantum technologies, 2017.

[170] V. Semenov, D.F. Schneider, J.C. Lin, and S. Polonsky. Interface between superconductor and semiconductor electronic circuits using phase-shift keying coded output data format, October 6 1998. US Patent 5,818,373.

[171] Ian Walmsley et al. NQIT Annual Report 2017, May 2017.

[172] Bjoern Lekitsch, Sebastian Weidt, Austin G Fowler, Klaus Mølmer, Simon J Devitt, Christof Wunderlich, and Winfried K Hensinger. Blueprint for a microwave trapped ion quantum computer. *Science Advances*, 3(2):e1601540, 2017.

[173] Jeremy L O'Brien, Geoffrey J Pryde, Andrew G White, Timothy C Ralph, and David Branning. Demonstration of an all-optical quantum controlled-not gate. *arXiv preprint quant-ph/0403062*, 2004.

[174] Terry Rudolph. Why i am optimistic about the silicon-photonic route to quantum computing. *APL Photonics*, 2(3):030901, 2017.

[175] Ryan Babbush, Peter J Love, and Alán Aspuru-Guzik. Adiabatic quantum simulation of quantum chemistry. *Scientific reports*, 4, 2014.

[176] JM Kreula, Stephen R Clark, and D Jaksch. Non-linear quantum-classical scheme to simulate non-equilibrium strongly correlated fermionic many-body dynamics. *Scientific reports*, 6:32940, 2016.

[177] Manabendra Nath Bera, Antonio Acín, Marek Kuś, Morgan Mitchell, and Maciej Lewenstein. Randomness in quantum mechanics: Philosophy, physics and technology. *arXiv preprint arXiv:1611.02176*, 2016.

[178] John M Rist. *Epicurus: an introduction*. CUP Archive, 1972.

[179] Antonio Acin. True quantum randomness. In Antoine Suarez and Peter Adams, editors, *Is science compatible with free will?: Exploring free will and consciousness in the light of quantum physics and neuroscience*, chapter 2, pages 7–22. Springer Science & Business Media, 2012.

[180] Roger Colbeck and Renato Renner. A systems wave function is uniquely determined by its underlying physical state. *New Journals of Physics*, 19(013016), 2017.

[181] John Stewart Bell. Bertlmann's socks and the nature of reality. In *Speakable and unspeakable in quantum mechanics: Collected papers on quantum philosophy*, chapter 16, pages 139–158. Cambridge university press, 2004.

[182] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[183] Mario Stipčević and Çetin Kaya Koç. True random number generators. In *Open Problems in Mathematics and Computational Science*, pages 275–315. Springer, 2014.

[184] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation. *npj Quantum Information*, 2:16021, 2016.

[185] Jürgen Audretsch. *Entangled systems: new directions in quantum physics*. John Wiley & Sons, 2008.

[186] Mario Stipcevic. Quantum random number generators and their use in cryptography. *arXiv preprint arXiv:1103.4381*, 2011.

[187] Matej Pivoluska, Martin Plesch, M Pivoluskaa, and M Plesch. Device independent random number generation. *Acta Physica Slovaca*, 64(6):601–664, 2014.

[188] http://www.idquantique.com/random-number-generation/.

[189] https://www.picoquant.com/products/category/quantum-random-number-generator/pqrng-150-quantum-random-number-generator.

[190] http://www.qutools.com/quRNG/.

[191] http://qrbg.irb.hr/.

[192] http://whitewoodsecurity.com/.

[193] https://www.quintessencelabs.com/products/qstream-quantum-true-random-number-generat

[194] https://qrng.anu.edu.au/.

[195] https://comscire.com/.

[196] Bruno Sanguinetti, Anthony Martin, Hugo Zbinden, and Nicolas Gisin. Quantum random number generation on a mobile phone. *Physical Review X*, 4(3):031056, 2014.

[197] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[198] Valerio Scarani. The device-independent outlook on quantum physics (lecture notes on the power of bell's theorem). *arXiv preprint arXiv:1303.3081*, 2013.

[199] Stefano Pironio, Valerio Scarani, and Thomas Vidick. Focus on device independent quantum information. *New Journal of Physics*, 18(10):100202, 2016.

[200] Antony Valentini. Signal-locality in hidden-variables theories. *Physics Letters A*, 297(5):273–278, 2002.

[201] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *arXiv preprint arXiv:0911.3814*, 2009.

[202] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by bell's theorem. *arXiv preprint arXiv:0911.3427*, 2009.

[203] Peter Bierhorst, Emanuel Knill, Scott Glancy, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, and Lynden K Shalm. Experimentally generated random numbers certified by the impossibility of superluminal signaling. *arXiv preprint arXiv:1702.05178*, 2017.

[204] Wikipedia. Counterfeit money. https://en.wikipedia.org/wiki/Counterfeit_money, 2017.

[205] Bitcoinwiki. How bitcoin works.

[206] Julio López and Ricardo Dahab. An overview of elliptic curve cryptography. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.2771, 2000.

[207] Wikipedia. Elliptic curve digital signature algorithm. https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm, 2017.

[208] Fernando Ulrich. O blockchain é incorruptível. https://www.youtube.com/watch?v=H9b8c0DxSSE, 2017.

[209] Adam Back. Hashcash - a denial of service counter-measure, 2002.

[210] B. Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. Wiley-India, 2007.

[211] Wikipedia. Sha-2. https://en.wikipedia.org/wiki/SHA-2, 2017.

[212] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

[213] Scott Aaronson, Edward Farhi, David Gosset, Avinatan Hassidim, Jonathan Kelner, and Andrew Lutomirski. Quantum money. *Commun. ACM*, 55(8):84–92, August 2012.

[214] Charles H. Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology: Proceedings of Crypto 82*, pages 267–275, Boston, MA, 1983. Springer US.

[215] S. Aaronson. Quantum copy-protection and quantum money. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 229–242, July 2009.

[216] A. Ambainis and J. Emerson. Quantum t-designs: t-wise independence in the quantum world. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 129–140, June 2007.

[217] A. Hayashi, T. Hashimoto, and M. Horibe. Reexamination of optimal quantum state estimation of pure states. *Phys. Rev. A*, 72:032325, Sep 2005.

[218] FM Ablayev and AV Vasiliev. Cryptographic quantum hashing. *Laser Physics Letters*, 11(2):025202, 2013.

[219] Yu-Guang Yang, Peng Xu, Rui Yang, Yi-Hua Zhou, and Wei-Min Shi. Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. *Scientific reports*, 6:19788 EP –, Jan 2016. Article.

[220] Pawan Sinha. Recognizing complex patterns. *nature neuroscience*, 5(11s):1093, 2002.

[221] Bruce MacLennan. *Gabor representations of spatiotemporal visual images*. University of Tennessee. Computer Science Department, 1991.

[222] Vernon B Mountcastle. The columnar organization of the neocortex. *Brain: a journal of neurology*, 120(4):701–722, 1997.

[223] Bernd Heisele, Purdy Ho, and Tomaso Poggio. Face recognition with support vector machines: Global versus component-based approach. In *Computer Vision, 2001. ICCV 2001. Proceedings. Eighth IEEE International Conference on*, volume 2, pages 688–694. IEEE, 2001.

[224] Matthew A Turk and Alex P Pentland. Face recognition using eigenfaces. In *Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91., IEEE Computer Society Conference on*, pages 586–591. IEEE, 1991.

[225] Peter N. Belhumeur, João P Hespanha, and David J. Kriegman. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. *IEEE Transactions on pattern analysis and machine intelligence*, 19(7):711–720, 1997.

[226] Daniel D Lee and H Sebastian Seung. Learning the parts of objects by non-negative matrix factorization. *Nature*, 401(6755):788, 1999.

[227] Daniel D Lee and H Sebastian Seung. Algorithms for non-negative matrix factorization. In *Advances in neural information processing systems*, pages 556–562, 2001.

[228] Fatma Zohra Chelali, A Djeradi, and R Djeradi. Linear discriminant analysis for face recognition. In *Multimedia Computing and Systems, 2009. ICMCS'09. International Conference on*, pages 1–10. IEEE, 2009.

[229] Nitin Bhatia et al. Survey of nearest neighbor techniques. *arXiv preprint arXiv:1007.0085*, 2010.

[230] Edgar Osuna, Robert Freund, and Federico Girosit. Training support vector machines: an application to face detection. In *Computer vision and pattern recognition, 1997. Proceedings., 1997 IEEE computer society conference on*, pages 130–136. IEEE, 1997.

[231] Teuvo Kohonen. The self-organizing map. *Neurocomputing*, 21(1):1–6, 1998.

[232] Teuvo Kohonen. Learning vector quantization. In *Self-Organizing Maps*, pages 175–189. Springer, 1995.

[233] David Guillamet and Jordi Vitria. Non-negative matrix factorization for face recognition. *CCIA*, 2:336–344, 2002.

[234] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *arXiv preprint arXiv:1611.09347*, 2016.

[235] Daniel O'Malley, Velimir V Vesselinov, Boian S Alexandrov, and Ludmil B Alexandrov. Nonnegative/binary matrix factorization with a d-wave quantum annealer. *arXiv preprint arXiv:1704.01605*, 2017.

[236] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. *arXiv preprint arXiv:1307.0401*, 2013.

[237] Patrick Rebentrost, Masoud Mohseni, and Seth Lloyd. Quantum support vector machine for big data classification. *Physical review letters*, 113(13):130503, 2014.

[238] Dan Ventura and Tony Martinez. Quantum associative memory. *Information Sciences*, 124(1):273–296, 2000.

[239] Maria Schuld, Ilya Sinayskiy, and Francesco Petruccione. Quantum computing for pattern classification. In *Pacific Rim International Conference on Artificial Intelligence*, pages 208–220. Springer, 2014.

[240] Alexy Bhowmick and Shyamanta M Hazarika. Machine learning for e-mail spam filtering: Review, techniques and trends. *arXiv preprint arXiv:1606.01042*, 2016.

[241] Ali Shafigh Aski and Navid Khalilzadeh Sourati. Proposed efficient algorithm to filter spam using machine learning techniques. *Pacific Science Review A: Natural Science and Engineering*, 18(2):145–149, 2016.

[242] Sohail Anwar. *Handbook of Research on Solar Energy Systems and Technologies*. IGI Global, 2012.

[243] Trevor B. Arp, Yafis Barlas, Vivek Aji, and Nathaniel M. Gabor. Natural regulation of energy flow in a green quantum photocell. *Nano Letters*, 16(12):7461–7466, 2016.

[244] Takeyoshi Sugaya, Osamu Numakami, Ryuji Oshima, Shigenori Furue, Hironori Komaki, Takeru Amano, Koji Matsubara, Yoshinobu Okano, and Shigeru Niki. Ultra-high stacks of ingaas/gaas quantum dots for high efficiency solar cells. *Energy & Environmental Science*, 5(3):6233–6237, 2012.

[245] JE Geusic, EO Schulz-DuBios, and HED Scovil. Quantum equivalent of the carnot cycle. *Physical Review*, 156(2):343, 1967.

[246] Konstantin E Dorfman, Dmitri V Voronine, Shaul Mukamel, and Marlan O Scully. Photosynthetic reaction center as a quantum heat engine. *Proceedings of the National Academy of Sciences*, 110(8):2746–2751, 2013.

[247] AP Kirk. Analysis of quantum coherent semiconductor quantum dot p- i- n junction photovoltaic cells. *Physical review letters*, 106(4):048703, 2011.

[248] Daryl M Chapin, CS Fuller, and GL Pearson. A new silicon p-n junction photocell for converting solar radiation into electrical power. *Journal of Applied Physics*, 25(5):676–677, 1954.

[249] Ulrike Woggon. *Optical properties of semiconductor quantum dots*. Springer, 1997.

[250] AJ Nozik. Quantum dot solar cells. *Physica E: Low-dimensional Systems and Nanostructures*, 14(1):115–120, 2002.

[251] Jun Du, Zhonglin Du, Jin-Song Hu, Zhenxiao Pan, Qing Shen, Jiankun Sun, Donghui Long, Hui Dong, Litao Sun, Xinhua Zhong, et al. Zn–cu–in–se quantum dot solar cells with a certified power conversion efficiency of 11.6%. *Journal of the American Chemical Society*, 138(12):4201–4209, 2016.

[252] F Dimroth. New world record for solar cell efficiency at 46%. *French-German cooperation confirms competitive advantage of European photovoltaic industry*, 1, 2014.

[253] Jean-Luc Brédas, Edward H Sargent, and Gregory D Scholes. Photovoltaic concepts inspired by coherence effects in photosynthetic systems. *Nature materials*, 16(1):35–44, 2017.

[254] Celestino Creatore, M Andy Parker, Stephen Emmott, and Alex W Chin. Efficient biologically inspired photocell enhanced by delocalized quantum states. *Physical review letters*, 111(25):253601, 2013.

[255] Artem A Bakulin, Akshay Rao, Vlad G Pavelyev, Paul HM van Loosdrecht, Maxim S Pshenichnikov, Dorota Niedzialek, Jérôme Cornil, David Beljonne, and Richard H Friend. The role of driving energy and delocalized states for charge separation in organic semiconductors. *Science*, 335(6074):1340–1344, 2012.

[256] Octavi E Semonin, Joseph M Luther, Sukgeun Choi, Hsiang-Yu Chen, Jianbo Gao, Arthur J Nozik, and Matthew C Beard. Peak external photocurrent quantum efficiency exceeding 100% via meg in a quantum dot solar cell. *Science*, 334(6062):1530–1533, 2011.

[257] Zerui Zheng, Haining Ji, Peng Yu, and Zhiming Wang. Recent progress towards quantum dot solar cells with enhanced optical absorption. *Nanoscale research letters*, 11(1):266, 2016.

[258] Smithsonian Institution. Origin of electrical power. http://americanhistory.si.edu/powering/past/prehist.htm, 2002.

[259] Jeff Desjardins. Explaining the surging demand for lithium-ion batteries. http://www.visualcapitalist.com/explaining-surging-demand-lithium-ion-batteries, 2016.

[260] Erwin Schrödinger. *What is life?: With mind and matter and autobiographical sketches*. Cambridge University Press, 1992.

[261] Robert Alicki, Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Thermodynamics of quantum information systems—hamiltonian description. *Open Systems & Information Dynamics*, 11(03):205–217, 2004.

[262] Armen E Allahverdyan, Roger Balian, and Th M Nieuwenhuizen. Maximal work extraction from finite quantum systems. *EPL (Europhysics Letters)*, 67(4):565, 2004.

[263] Robert Alicki and Mark Fannes. Entanglement boost for extractable work from ensembles of quantum batteries. *Physical Review E*, 87(4):042123, 2013.

[264] Felix C Binder, Sai Vinjanampathy, Kavan Modi, and John Goold. Quantacell: powerful charging of quantum batteries. *New Journal of Physics*, 17(7):075015, 2015.

[265] Francesco Campaioli, Felix A Pollock, Felix C Binder, Lucas Céleri, John Goold, Sai Vinjanampathy, and Kavan Modi. Enhancing the charging power of quantum batteries. *Physical Review Letters*, 118(15):150601, 2017.

[266] Alexander Niggebaum. *Towards mobile quantum sensors for gravity surveys*. PhD thesis, University of Birmingham, 2016.

[267] Michel Van Camp, Simon DP Williams, and Olivier Francis. Uncertainty of absolute gravity measurements. *Journal of Geophysical Research: Solid Earth*, 110(B5), 2005.

[268] Zhiheng Jiang, V Pálinkáš, Olivier Francis, Philippe Jousset, J Mäkinen, Sébastien Merlet, Markus Becker, A Coulomb, KU Kessler-Schulz, HR Schulz, et al. Relative gravity measurement campaign during the 8th international comparison of absolute gravimeters (2009). *Metrologia*, 49(1):95, 2011.

[269] TT In. Fundamental parameters and current (2004) best estimates of the parameters of common relevance to astronomy, geodesy, and geodynamics. *Journal of Geodesy*, 2004.

[270] Achim Peters, Keng Yeow Chung, and Steven Chu. High-precision gravity measurements using atom interferometry. *Metrologia*, 38(1):25, 2001.

[271] RP Middlemiss, Antonio Samarelli, DJ Paul, James Hough, Sheila Rowan, and GD Hammond. Measurement of the earth tides with a mems gravimeter. *Nature*, 531(7596):614–617, 2016.

[272] Jongmin Lee. Spring gravimeters and other alternatives. http://large.stanford.edu/courses/2007/ph210/lee1/.

[273] Jia Ai-Ai, Yang Jun, Yan Shu-Hua, Hu Qing-Qing, Luo Yu-Kun, and Zhu Shi-Yao. Wave–particle duality in a raman atom interferometer. *Chinese Physics B*, 24(8):080302, 2015.

[274] M Hauth, C Freier, V Schkolnik, A Senger, M Schmidt, and A Peters. First gravity measurements using the mobile atom interferometer gain. *Applied Physics B*, 113(1):49–55, 2013.

[275] Christian Freier, Matthias Hauth, Vladimir Schkolnik, Bastian Leykauf, Manuel Schilling, Hartmut Wziontek, Hans-Georg Scherneck, Jürgen Müller, and Achim Peters. Mobile quantum gravity sensor with unprecedented stability. In *Journal of Physics: Conference Series*, volume 723, page 012050. IOP Publishing, 2016.

[276] Mark Kasevich, David S Weiss, Erling Riis, Kathryn Moler, Steven Kasapi, and Steven Chu. Atomic velocity selection using stimulated raman transitions. *Physical review letters*, 66(18):2297, 1991.

[277] Andrew A Geraci and Andrei Derevianko. Sensitivity of atom interferometry to ultralight scalar field dark matter. *Physical review letters*, 117(26):261301, 2016.

[278] Jonas Hartwig, Sven Abend, Christian Schubert, Dennis Schlippert, Holger Ahlers, Katerine Posso-Trujillo, Naceur Gaaloul, Wolfgang Ertmer, and Ernst Maria Rasel. Testing the universality of free fall with rubidium and ytterbium in a very large baseline atom interferometer. *New Journal of Physics*, 17(3):035011, 2015.

[279] Anne Louchet-Chauvet, Tristan Farah, Quentin Bodart, André Clairon, Arnaud Landragin, Sébastien Merlet, and Franck Pereira Dos Santos. The influence of transverse motion within an atomic gravimeter. *New Journal of Physics*, 13(6):065025, 2011.

[280] DN Aguilera, H Ahlers, Baptiste Battelier, A Bawamia, Andrea Bertoldi, R Bondarescu, K Bongs, Philippe Bouyer, C Braxmaier, L Cacciapuoti, et al. Ste-quest—test of the universal-

ity of free fall using cold atom interferometry. *Classical and Quantum Gravity*, 31(11):115010, 2014.

[281] Esmond Mok, Guenther Retscher, and Chen Wen. Initial test on the use of gps and sensor data of modern smartphones for vehicle tracking in dense high rise environments. In *Ubiquitous Positioning, Indoor Navigation, and Location Based Service (UPINLBS), 2012*, pages 1–7. IEEE, 2012.

[282] Total number of websites. http://www.internetlivestats.com/total-number-of-websites/, 2016.

[283] IBM M. Tim Jones, developer Works. Recommender systems, part 1: Introduction to approaches and algorithms. https://www.ibm.com/developerworks/library/os-recommender1/, 2013.

[284] Ivens Portugal, Paulo Alencar, and Donald Cowan. The use of machine learning algorithms in recommender systems: a systematic review. *arXiv preprint arXiv:1511.05263*, 2015.

[285] The netflix prize. http://www.netflixprize.com/, 2009.

[286] Indranil Chakrabarty, Shahzor Khan, and Vanshdeep Singh. Dynamic grover search: applications in recommendation systems and optimization problems. *Quantum Information Processing*, 16(6):153, 2017.

[287] Lov K Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 79(2):325, 1997.

[288] Hamming distance. https://en.wikipedia.org/wiki/Hamming_distance, 2017.

[289] Jeff Tyson and Tracy V. Wilson. How graphics cards work. http://computer.howstuffworks.com/graphics-card1.htm, 2017.

[290] David P. Rodgers. Improvements in multiprocessor system design. *SIGARCH Comput. Archit. News*, 13(3):225–231, June 1985.

[291] Wikipedia. Amdahl's law. https://en.wikipedia.org/wiki/Amdahl%27s_law, 2017.

[292] Salvador E Venegas-Andraca and JL Ball. Processing images in entangled quantum systems. *Quantum Information Processing*, 9(1):1–11, 2010.

[293] Salvador Venegas-Andraca and Sougato Bose. Storing, processing and retrieving an image using quantum mechanics. *Proceedings of SPIE - The International Society for Optical Engineering*, 5105, 08 2003.

[294] Jose I. Latorre. Image compression and entanglement. *arXiv:quant-ph/0510031*, 2005.

[295] Phuc Q. Le, Fangyan Dong, and Kaoru Hirota. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. *Quantum Information Processing*, 10(1):63–84, Feb 2011.

[296] Simona Caraiman and Vasile I. Manta. Image segmentation on a quantum computer. *Quantum Information Processing*, 14(5):1693–1715, May 2015.

[297] Marco Lanzagorta and Jeffrey K. Uhlmann. Hybrid quantum-classical computing with applications to computer graphics. In *ACM SIGGRAPH 2005 Courses*, SIGGRAPH '05, New York, NY, USA, 2005. ACM.

[298] S Caraiman. Towards quantum computer graphics. In *Proceedings of the 14th International Conference on System Theory and Control*, pages 17–19, 2010.

[299] Marco Lanzagorta and Jeffrey K. Uhlmann. Quantum computational geometry. In *Proc. SPIE*, volume 5436, pages 332–339, 2004.

[300] Simona Caraiman and Vasile I. Manta. New applications of quantum algorithms to computer graphics: The quantum random sample consensus algorithm. In *Proceedings of the 6th ACM Conference on Computing Frontiers*, CF '09, pages 81–88, New York, NY, USA, 2009. ACM.