



University of  
BRISTOL



## QUANTUM ENGINEERING CENTRE FOR DOCTORAL TRAINING

---

### Quantum at Home

---

COHORT III

UNIVERSITY OF BRISTOL

August 2017

## **Abstract**

We made up some stuff about how quantum might be used by everyday people.

# Contents

<b>Acronyms</b>	viii
<b>1 Introduction</b>	1
<b>2 Health</b>	1
<b>3 Security</b>	2
<b>4 Environment</b>	3
<b>5 Entertainment</b>	3
<b>6 Productivity</b>	4
<b>7 Conclusion</b>	4
<b>A Quantum Netflix</b>	5
A.1 Introduction . . . . .	5
A.1.1 Collaborative filtering . . . . .	5
A.1.2 . . . . .	5
<b>B Quantum Random Number Generation</b>	6
B.1 Randomness in Classical and Quantum Physics . . . . .	6
B.2 Random numbers in practice . . . . .	6
B.3 The superior Device-Independent approach . . . . .	7
<b>C Quantum Processor</b>	9
C.1 Introduction . . . . .	9
C.2 Classical . . . . .	9
C.3 Quantum . . . . .	10
C.4 Discussion . . . . .	10
<b>D Quantum Video Games</b>	11
D.1 Introduction . . . . .	11
D.2 Classical Video Game . . . . .	11
D.2.1 The GPU . . . . .	11
D.3 A Quantum Video Game . . . . .	12
D.3.1 The Algorithm Approach . . . . .	12
D.3.2 The Hardware Approach . . . . .	14

<b>E Quantum Enhanced Cameras</b>	<b>16</b>
E.1 Introduction . . . . .	16
E.2 The Classical Version . . . . .	16
E.2.1 Light Sources . . . . .	16
E.2.2 Cameras and the Diffraction Limit . . . . .	17
E.3 The Quantum Counterpart . . . . .	18
E.3.1 Entangled Photons and Beyond the Diffraction Limit . . . . .	18
E.3.2 Squeezed Light . . . . .	19
E.4 Applications . . . . .	19
<b>F Quantum Enhanced Solar Cells</b>	<b>21</b>
F.1 Comparison to Current Techniques . . . . .	21
F.2 The Quantum Enhanced Photocell . . . . .	21
F.3 Nature-inspired Quantum Alternatives . . . . .	23
<b>G Quantum Enhanced Material Detection</b>	<b>24</b>
<b>H Quantum Battery</b>	<b>25</b>
H.1 Classical . . . . .	25
H.2 Quantum . . . . .	26
H.3 Discussion . . . . .	27
<b>I Gravity Sensors</b>	<b>28</b>
I.1 Classical . . . . .	29
I.1.1 Spring . . . . .	29
I.1.2 Superconducting . . . . .	30
I.1.3 Free-fall . . . . .	30
I.2 Quantum . . . . .	30
I.2.1 Examples: Very Long Baseline Atom Interferometry and Atom Chip Interferometry . . . . .	33
I.3 Discussion . . . . .	33
<b>J Quantum Magnetic Sensors</b>	<b>35</b>
J.1 Introduction . . . . .	35
J.2 The Current Technology . . . . .	35
J.3 Quantum Enhanced Magnetic Sensing . . . . .	35
J.4 Applications . . . . .	38
<b>K Quantum Dots for Biosensors and Chemical Sensors</b>	<b>40</b>
K.1 Classical . . . . .	40
K.2 Quantum . . . . .	40
K.3 Discussion . . . . .	41

<b>L Quantum Money</b>	<b>44</b>
L.1 Introduction . . . . .	44
L.2 Classical . . . . .	44
L.2.1 Paper Money . . . . .	44
L.2.2 Cryptocurrencies . . . . .	45
L.3 Quantum . . . . .	48
L.3.1 Paper Money . . . . .	48
<b>M Quantum Pattern Matching</b>	<b>49</b>
M.1 Introduction . . . . .	49
M.2 Classical . . . . .	49
M.3 Quantum . . . . .	51
M.4 Discussion . . . . .	52
<b>N Superman Memory Crystal</b>	<b>54</b>
<b>O Quantum Teleportation</b>	<b>55</b>
<b>P Handheld Authenticator</b>	<b>56</b>
P.1 Classical . . . . .	56
P.2 Quantum . . . . .	56
P.3 Discussion . . . . .	57
P.3.1 Short Term . . . . .	57
P.3.2 Long term . . . . .	59
P.3.3 Other potential uses . . . . .	59
<b>Q Optical Port and Router</b>	<b>60</b>
Q.1 Classical . . . . .	60
Q.2 Quantum . . . . .	60
Q.3 Discussion . . . . .	61
Q.3.1 Quantum Routers . . . . .	61
Q.3.2 Quantum Key Distribution . . . . .	62
Q.3.3 Blind Quantum Computing . . . . .	63
<b>R Quantum Simulation</b>	<b>64</b>
R.1 Classical . . . . .	64
R.1.1 Monte Carlo Simulations . . . . .	64
R.2 Quantum . . . . .	65
R.2.1 Analog Quantum Simulations . . . . .	65
R.2.2 Digital Quantum Simulations . . . . .	66
R.2.3 Electronics . . . . .	66
R.2.4 Drugs and medicine . . . . .	67

# List of Tables

# List of Figures

A.1	Collaborative recommendation systems compares two similar users and picks recommendations from the differences between them. . . . .	5
D.2	A sketch of a GPU with some of its components. . . . .	12
D.3	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). . . . .	13
D.4	Example of a simple $2 \times 2$ quantum image with four possible colors (two qubits are used to represent the color information and two qubits encode the position of each pixel. . . . .	15
E.5	Different features for classifying light. Taken from [1]. . . . .	17
E.6	Basic elements of a modern camera. . . . .	18
E.7	Quadrature squeezed states. The dotted circle in each of the diagrams shows the quadrature uncertainty of the states with $\Delta X_1 = \Delta X_2 = 1/2$ . Taken from [1]. . . .	20
F.8	(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 $\gamma_a$ and $\gamma_b$ respectively. The output energy is given by $E_M$ and is characterised by the rate of relaxation $\Gamma$ from state $ x\rangle$ to state $ y\rangle$ . $\gamma_g$ represents the rate of decay to the ground state $ g\rangle$ [2]. . . . .	22
H.9	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. This image is taken from [3] where they showed that the correlations between the qubits affect the charging power when the system is drove globally. . . . .	26
I.10	Precision of gravity sensing . . . . .	28
I.11	Acceleration due to various masses . . . . .	29
I.12	Free-fall corner cube . . . . .	30
I.13	Atomic interferometry . . . . .	31
I.14	Atomic interferometer . . . . .	31
I.15	Path divergence in atomic interferometry . . . . .	32

J.16	(a) Photograph of the microfabricated optical magnetometer sensor in [4]. The size of the sensor head is approximately 0.36cm. 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. . . . .	36
J.17	Diagram of the experimental apparatus for a typical QND atomic magnetometer as in [5]. A pump laser is used to spin polarize the atomic vapour, and a linearly polarized 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. . . . .	36
J.18	Schematic of the diamond-based scanning spin microscope in [6]. 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 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. . . . .	37
J.19	This schematic illustrates a bulk dimaond magnetometer with a high density of NV centres for sensing fields created by remote objects, as proposed in [7]. Here, a laser beam directed onto the sample induces spin-dependent photoluminescence, which can be detected using a CCD. . . . .	38
K.20	Illustration of colour/size relationship of quantum dots . . . . .	41
K.21	Detection differentiation of explosive chemicals using quantum dots . . . . .	42
L.22	Anti-counterfeiting features on an old U.S. \$20 bill. . . . .	46
L.23	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. . . . .	47
P.24	BB84 Protocol . . . . .	57
P.25	4 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 [8] . . . . .	58
P.26	Schematic of the receiving device used to perform handheld QKD. Image provided by David Lowndes . . . . .	58
P.27	Photos of the transmitting (left) and receiving (right) devices used to perform handheld QKD. Image provided by David Lowndes . . . . .	58

Q.28	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 [9] . . . . .	61
Q.29	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 [10] . . . . .	62
Q.30	Basic Idea of the BB84 QKD 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 [11] . . . . .	63

## **Acronyms**

**AQS** Analog Quantum Simulation.

**ATM** Automated Teller Machine.

**CAP/DPA** Chip Authentication Program/Dynamic Passcode Authentication.

**COW** Coherent One Way.

**DQS** Digital Quantum Simulation.

**EFTPOS** Electronic Funds Transfer at Point of Sale.

**GDP** Gross Domestic Product.

**iTAN** indexed Transaction Authentication Numbers.

**LAN** Local Area Network.

**LEDs** Light Emitting Diodes.

**OFDM** Orthogonal Frequency Division Multiplexing.

**QC** Quantum Computing.

**QKD** Quantum Key Distribution.

**QRNG** Quantum Random Number Generators.

**RNG** Random Number Generator.

**WEF** World Economic Forum.

**WEP** Wired Equivalent Privacy.

**WPA** Wi-Fi Protected Access.

# 1 Introduction

In the 20th century myriad quantum technologies changed the way we lived our day-to-day lives, most notably the microprocessor: the electronic properties of semiconductors are described by quantum mechanics. Today, another wave of quantum technologies are making their way out of the lab. 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.

Physical devices designed to exploit the abstract ideas of quantum mechanics show promise to supersede current technologies in fields far-ranging, diverse and influential such as computing, communication, health, science, navigation, security, imaging, entertainment and sensing.

Around the world there are notable initiatives driving forward quantum technologies, which in the field of quantum computation has been likened to an arms race [12]. In China, the 2016–2020 5-year plan lists quantum communications and computing as one of five top priorities for development [13]. In America, though government investment in science is dropping [14], 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 driving through the QC revolution most notably in defence and intelligence [15].

Flagship projects in the UK (£270 million [16]) and the EU (€1 billion [17]) are comparable to the other grand scientific projects of our time: mapping the human brain, graphene and fusion. Globally in 2015, there were around 7000 researchers with an annual expenditure of \$1.5 billion [18].

This collection of essays aims to highlight how these technologies will influence our day-to-day lives, how quantum mechanics is being used to create new technologies that are pushing the frontiers of science, and will end up in our homes.

# 2 Health

In the UK expenditure on health is rising as a proportion of Gross Domestic Product (GDP) [19]; notably in developed economies, population demographics are getting older [20], new drugs are costly to develop and trial [21], 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” [22]. Here, we define healthcare as the tools for diagnosis and treatment of disease, and 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 [23] 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 R, 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, stability and decrease the cost, even to the extent that currently prohibitively expensive devices, such as MRI machines, could be used in house, Article J.

Finally, quantum enhanced cameras, by exceeding the classical diffraction limit, can offer cheaper and more sensitive ways to image microscopic biological structures with more resolution than is available in current optical imaging devices, Article E.

### 3 Security

Our lives have shifted into the digital space. We now shop, bank, play, work and communicate online. The compromise between privacy and security is one of the big ethical debates of the 21st century [24]. In a survey conducted by Pew Research Centre 86% of respondents claimed to have taken steps to avoid surveillance online [25].

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 [26] and systems integrated on silicon [27] are bringing the field closer to widespread commercial adoption.

QKD has applications that are local in day-to-day life, for example, locks for cars Article P, secure contactless payments and quantum ATMs. Less locally but no less important is the application to backbone networks for secure key distribution consisting of QKD nodes, alike to current communications networks, Article Q.

Further, the intrinsic and true randomness of quantum systems can be used in random number generation. Quantum Random Number Generator (RNG)s promise to be certifiable, private and device independent, with applications in cryptography, Article B.

## 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 [28]. The recently signed Paris climate accord is culturally and politically a step forward [29].

Parallel to these policy steps, technology is beginning to tackle the problems of pollution and over-consumption. Specifically, though not limited to, in the fields of battery technology and solar energy quiet revolutions are taking place: in 2015 the cost of batteries was set to plunge by a half by 2019 [30] and in 2016 the WEF found that the cost of introducing new solar capacity was the same cost or cheaper than for fossil fuels [31].

These revolutions will change the way we use and distribute power, and may be influenced by the quantum technologies for applications in solar energy, Appendix F, and batteries, Appendix H.

Additionally to these examples, for locating resources, detecting sinkholes, climate research and geology, advances in quantum gravity sensors may soon exceed their classical counterparts in cost, sensitivity and mobility, Appendix I.

## 5 Entertainment

Technology has changed the way we entertain ourselves: the television (cathode ray) and computers (microprocessor) are clear examples of this. As discussed in Section 3, Quantum Random Number Generators (QRNG)s offer true randomness, which could easily be applied as the basis of fair and verifiably random online gambling, Appendix B.

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, Appendix J, and high resolution cameras, Appendix E.

Perhaps the most challenging and exciting quantum revolution will be in computing. The development of the theory of quantum information processing has encouraged commercial drive for quantum computation for applications in science and industry. In the future, these devices may be used as hybrid quantum classical computation systems to deliver more computing power available to individuals, either at physically at home or in the quantum cloud, Appendix C.

## 6 Productivity

Innovation and productivity in business are intimately linked [32]. New technology, generally, offers some advantage in productivity or use of resource. Quantum technologies promises to influence the productivity of business and individuals.

In another field, machine learning, another technological leap forward is taking place that will change the socioeconomic landscape and permeate our lives from self-driving cars [33] to personal assistants. Quantum machine learning shows promise to one day increase the speed of learning algorithms, for applications such as facial recognition and optimisation problems, Appendix M.

Other advances include the ability to detect chemicals in recycling waste, Appendix K, applications of quantum clocks in navigation and finance, Appendix ??.

Further, with quantum devices poised to replace their classical counter parts in ability to deploy, cost and size we may see advanced quantum technologies replacing classical devices in applications as local and meaningful as house restoration, as in the case of gravity sensing, Appendix I, with wider reaching application in construction and infrastructure.

## 7 Conclusion

# A Quantum Netflix

## A.1 Introduction

HOW RECOMMENDATION ALGORITHMS AFFECT OUR LIFE?

HOW DOES RECOMMENDATION ALGORITHMS WORK?

[34]

Basic approaches. Most recommender systems take either of two basic approaches: collaborative filtering or content-based filtering.

### A.1.1 Collaborative filtering

In collaborative filtering the system generates recommendations using explicit or implicit preferences from many users ignoring the items representation. These systems recommend items based on similarity measures between users and/or items. The items recommended to a user are those preferred by similar users.

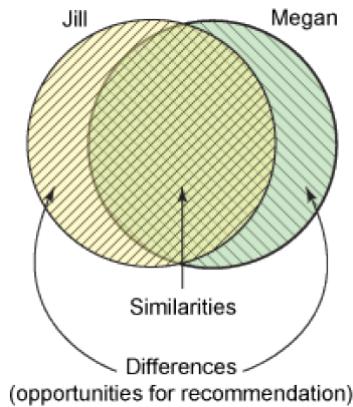


Figure A.1: Collaborative recommendation systems compares two similar users and picks recommendations from the differences between them.

### A.1.2

IS THIS MACHINE LEARNING?

HOW CAN QUANTUM IMPROVE THIS? (QUANTUM ML OR GROVERS ALGORITHM)  
quantum recommendation algorithm [35]

## B Quantum Random Number Generation

### B.1 Randomness in Classical and Quantum Physics

Randomness is an exciting concept. Since the period of Epicurus and Democritus there has been a discussion about whether nature is deterministic or not [36,37]. Within the framework of classical physics there is no real randomness. The probabilities appeared 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” [1]. Imagine for example the experiment of flipping a coin. If we knew exactly the initial conditions of the motion of the dice and of the air molecules, then, according to the laws of classical mechanics, we would predict the outcome with absolute certainty [38,39]. 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! [3]. This is the so called “fundamental”, “ontic”, “intrinsic” or “inherent” randomness. This is the kind of randomness that annoyed Einstein who supported that “God does not play dice” [40][3,5]. Following Einstein’s ideas John Bell produced the experimentally testable “Bell inequality” the violation of which reveals if God plays dice! [5,6] Below we shall see why this new kind of randomness is useful for technological purposes.

### B.2 Random numbers in practice

Random numbers are useful in many applications such as cryptography, randomized polling, lotteries, gaming and gambling, industrial testing and labeling, computer simulations of complex physical, chemical, biological, social and economical systems etc [1,7]. There are three types of random number generators (RNG), the pseudo-RNG, the “true” RNG and the quantum RNG [3]. 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” [7,8]. Indeed, pseudo-random number sequences suffer from long-range correlations that undermine cryptographic strength and produce errors in Monte Carlo simulations [23]. The “true” RNG use 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. Finally, the quantum RNGs utilize genuine quantum features to generate random bits. In the cases of both classical and quantum cryptography the existence of a “good” RNG is vital. The applications of cryptography to our everyday life are numerous: online payments, ATM’s, e-banking, wireless keys, e-mail access, mobile communications etc [7]. In simple words 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 [20,22]. 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 [1]. 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. In contrast, if there are physical procedures intrinsically random then unconditional secure coding schemes and unconditionally fair gaming schemes are doable [1]. The figure below shows an optical quantum system used to generate random numbers. A single photon is sent towards a semitransparent mirror (beam 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 [1] and the internal working of the semitransparent mirror [10,24] we can claim that which detector will click is a fundamentally unpredictable event. This apparatus is one of the commercially popular and successful quantum RNG [ID-quantique, 8,9] So far there are many patents for QRNG available either in the market or online for free use [10]. They use principles of quantum systems such as photon arrival times [PicoQuant, 11, Qutools, 12], photon emission in semiconductor LED diodes [QBG121,13], photon bunching [Whitewood,14], electron-hole pair generation in a semiconductor [MPD,15], measurement of quantum noise at high frequencies [Quintessencelabs,16], measurement of quantum fluctuations of the vacuum [ANU, 17] and shot noise based [Comscire,18]. Apart from these technologies it is remarkable that scientists have proposed a QRNG based on accessories almost available in our mobile phones! [19] The quality of the cameras integrated in mobile phones has improved in such extent so 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 [20]. 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! [23]

### B.3 The superior Device-Independent approach

But can we believe a quantum RNG if quantum theory is not the final theory of the universe, 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 gives answers to these questions introducing the new field of the device independent quantum random number generation (DI-QRNG). The device independent approach deals even with the worst imaginable paranoid-minded [10] 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 [23]. 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 [3,24]. The fact that the input-output statistics of these boxes violate certain kind of inequalities, the Bell-type inequalities, can certify that the inner working of these black-boxes is fundamentally random [24]. This new field of quantum RNG utilizes the fundamental Valentini’s theorem which says that

“Nonlocal correlations plus Determinism implies Signaling” [3,21]. No-signaling, 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 approach is that the black-box output must be random otherwise some fundamental physical law must be broken [10]. The DI method promises randomness which is [1,3] • 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 modeling of the internal working principles of the experimental devices and thus it is robust to imperfect or malicious devices. In our days, the efforts for a device independent quantum RNG are not in a theoretical but in an experimental stage [25,26]. In the upcoming “quantum at home” era quantum RNG will provide unbreakable and secure passwords wherever are necessary: In home security systems, in our strongboxes, in our transactions and in our entertainment and investments with fair gaming and gambling.

## C Quantum Processor

### C.1 Introduction

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 graphical 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 impossible 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 [41] on using the D-Wave machine as a quantum boltzmann machine could lead to a QPU specialised into certain machine learning applications.

### C.2 Classical

A modern classical computer divides the work it does between the 2 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 5nm transistor [42]) 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 its 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 (though 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 parrallelism 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 independant of each other but this happens fairly often in computing and hence GPUs form an essential part of a modern PC.

### **C.3 Quantum**

### **C.4 Discussion**

## D Quantum Video Games

### D.1 Introduction

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 USD 74 billion 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 developing and improving games.

### D.2 Classical Video Game

A classical video game console nowadays heavily depends on a graphics processing unit (GPU). A GPU is a specialized 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 GPU’s. In the following we shall describe a GPU more carefully.

#### D.2.1 The GPU

A processing graphics card is a printed circuit board that houses a processor and 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 that are necessary for graphics rendering. To improve image quality, the processors use:

- Full scene anti aliasing (FSAA), which smoothes the edges of 3-D objects
- Anisotropic filtering (AF), 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 color 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, called the DAC. This converter, also called the RAMDAC, translates the image into an analog signal that the monitor can use. Some cards have multiple RAMDACs, which can improve performance and support more than one monitor.

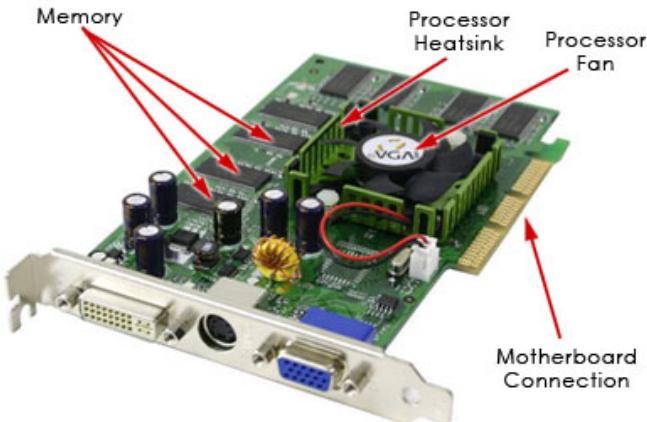


Figure D.2: A sketch of a GPU with some of its components.

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: 3-D 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 rasterize the image.

## D.3 A Quantum Video Game

How can then the quantum technologies improve the video games performance? And which features or components of a video game will be improved? In this section we shall explore two possible approaches for these questions. The first one will be an algorithm approach. We will discuss the possibility of a video game being based on quantum algorithms. In other words, if the coding on which the game is based can be translated to an equivalent quantum coding. And the second approach will be a hardware approach. We shall debate if 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.

### D.3.1 The Algorithm Approach

One way forward would be creating specific algorithms for the games themselves. As just mentioned, can the code lines of the game be performed in a quantum manner? Even though 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 accordingly 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. First, if the performed task falls 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 (GNFS) 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.

Second, even if a given task within the game can be substantially improved with a quantum algorithm, it does not mean that the whole program, or the whole game, will present a substantial speedup. This particularity is depicted by the Amdahl's law [43], which 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 (D.3)). The unimprovable part of the game will greatly limit the quantum speedup.

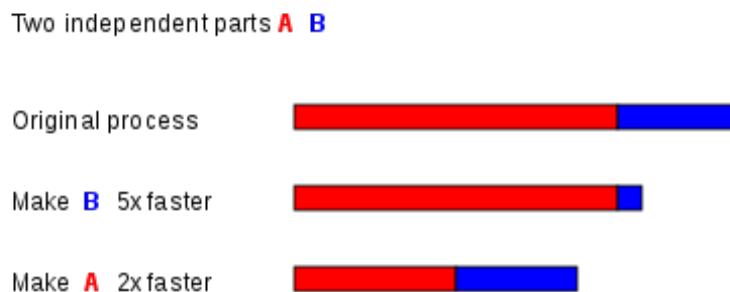


Figure D.3: Assume that a task has two independent parts, A and B. Part B takes roughly 25% of the time of the whole computation. By working very hard, one may be able to make this part 5 times faster, but this reduces the time of the whole computation only slightly. In contrast, one may need to perform 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).

Third, this tasks will require a quantum computer to run. To have 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 then aim at a general and important task that could be greatly improved by quantum technology. This leads us to the next approach.

### D.3.2 The Hardware Approach

Another approach, different from the game one described above, would be a output or hardware approach. As mentioned when describing the classical video game, it heavily depends on a graphics processing unit (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 having an improvement 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 has already interesting quantum algorithms for particular problems and also proposals for quantum image representation, e.g. Qubit Lattice [44,45], Real Ket [46] and Flexible Representation of Quantum Images (FRQI) [47]. As an example, one of the ideas to represent a quantum image it 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 color and position information. Pixel positions are coded in  $|P\rangle$  using  $2n$  qubits (is it possible to encode the information using qutrits, i.e. three level systems). The color information of a single pixel is encoded using a single qubit [45,47]:

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

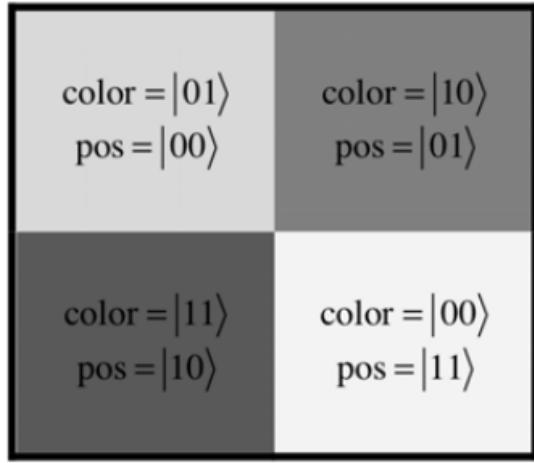
The real parameter encodes the frequency of the electromagnetic wave while is left uninitialized. Therefore our total state is

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

Coefficients  $\alpha_{ij}$ , 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 color of a pixel with position  $i$  by means of a superposition of all possible colors. For a given pixel  $i$ , coefficients  $\alpha_{ij}$  take value 1 if the color of the pixel is  $j$ , and 0 otherwise. This is illustrated in Fig. (D.4) with a simple example of a  $2 \times 2$  image with four colors.

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, which represents the relative frequency of occurrence of the various colors (gray levels) in the image.

Regarding the quantum algorithms for particular problems related to image processing, a few quantum algorithms have been suggested for the rendering problem [48,49] and computational geometry [50]. Even the important task of image segmentation found an quantum analogue based on quantum circuit schemes [51], as well as the classical RANSAC algorithm (RANdom SAmple Consensus voting scheme), vital for fundamental matrix estimation, trifocal tensor estimation, camera pose estimation, structure from motion and shape detection, was translated into a quantum version [52]. This translation was done by identify the RANSAC algorithm as a search algorithm, which



$$\begin{aligned}
|Q\rangle &= \frac{1}{\sqrt{2^2}} \sum_{i=0}^{2^2-1} \sum_{j=0}^{2^2-1} \alpha_{ij} |j\rangle|i\rangle = \\
&= \frac{1}{\sqrt{2^2}} (|01\rangle|00\rangle + |10\rangle|01\rangle + |11\rangle|10\rangle + |00\rangle|11\rangle) \\
\alpha_{00} &= 0, \alpha_{01} = 1, \alpha_{02} = 0, \alpha_{03} = 0 \\
\alpha_{10} &= 0, \alpha_{11} = 0, \alpha_{12} = 1, \alpha_{13} = 0 \\
\alpha_{20} &= 0, \alpha_{21} = 0, \alpha_{22} = 0, \alpha_{23} = 1 \\
\alpha_{30} &= 1, \alpha_{31} = 0, \alpha_{32} = 0, \alpha_{33} = 0
\end{aligned}$$

Figure D.4: Example of a simple  $2 \times 2$  quantum image with four possible colors (two qubits are used to represent the color information and two qubits encode the position of each pixel).

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 at the task of building a quantum computer, which by itself is an amazing challenge. On one hand, it is possible, though, that a quantum system focused solely on graphics issues might be required, therefore it can be possible to have quantum technologies impacting the video games industry before the advent of full quantum computer. On the other hand, the algorithms aforementioned may require an universal quantum machine to carry on all the calculations. Nonetheless, quantum technologies will probably find applications in the video game industry, not in the development of games itself, but in external, and highly parallelized, tasks such as image processing.

# E Quantum Enhanced Cameras

## E.1 Introduction

Along 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. Differently from the previous light sources, like the light bulb, which emit thermal light, i.e. the atoms in such sources radiate independently, with no relationship between the phases for independent atom, the laser represented a huge breakthrough regarding light sources because it emits a distinct type of light, called coherent. 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 on medical areas. Straightforward examples are cancer diagnosis [53], cancer treatment [54], melanoma treatment to scar revision, skin resurfacing, laser hair removal, tattoo removal [55].

Similar to creating light, mankind has a long history of detecting it. Having already our basic and natural light detector, the eye, men later developed the camera and the camera photo in 1826, which allowed us to store light information (not the light itself) into images. Since then, better and better cameras were developed. Now companies deliver professional cameras and cellphones with better resolution and characteristics, e.g. anti-blur modes, various focal planes, FOV.

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

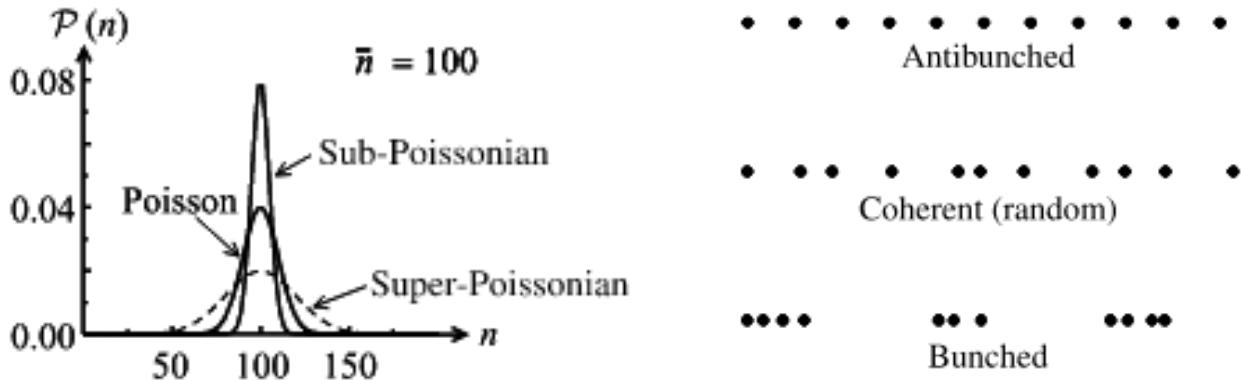
## E.2 The Classical Version

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

### E.2.1 Light Sources

A light source can be characterise by the light it emits. As mentioned before, there are classical sources like the light bulb, which emit thermal light, i.e. the atoms in such sources radiate independently, with no relationship between the phases for independent atom, and classical light sources like the laser that emit coherent light, which occurs when the atoms radiate with a constant phase difference and the same frequency. There are ways of classifying these light sources by some of their properties. The first we mention is by photon statistics.

Light can be thought of being made up by photons. If we take different parts of the light wave, the number of photons in it will fluctuate around a certain mean  $\bar{n}$ . This fluctuation is expressed by the standard deviation  $\Delta n$ . Light is classified depending how large is  $\bar{n}$  compared to  $\Delta n$ . 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 E.5: Different features for classifying light. Taken from [1].

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

The thermal light has super-Poissonian statistics, while the laser has Poissonian statistics. The sub-Poissonian statistics is thus characterised 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, to find the statistical character of intensity fluctuations. It is defined as [1]

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

Informally, the degree of coherence  $g^{(2)}$  measures how bunched the photons are (see Figure (E.5)). 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 thus a purely quantum optical phenomenon.

### E.2.2 Cameras and the Diffraction Limit

In 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 (E.6)). A shutter mechanism controls the length

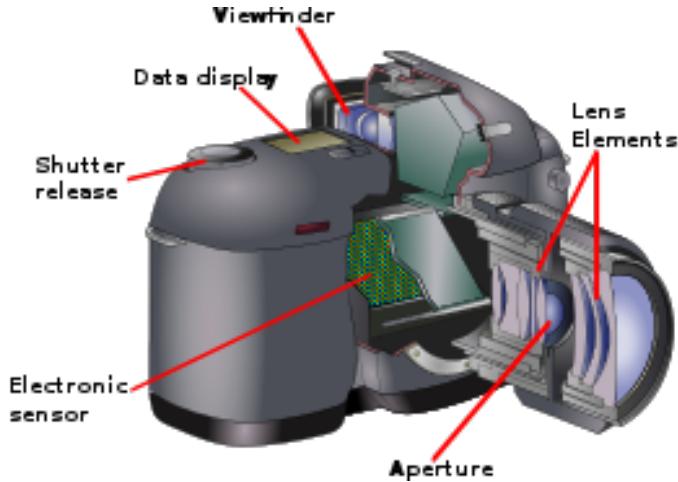


Figure E.6: Basic elements of a modern camera.

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 classical, 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, which is called the diffraction limited. The diffraction limit can be 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

$$\xi_{classical} = 0.61\lambda LR.$$

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

## E.3 The Quantum Counterpart

One characteristic that quantum technologies can improve when it comes to cameras is their resolution, i.e. the diffraction limit. This in turn 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.

### E.3.1 Entangled Photons and Beyond the Diffraction Limit

Entanglement is one of the most striking features from quantum mechanics and that 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  $|\psi\rangle_A \times |\phi\rangle_B$ . But it can be the case where the state of the whole system  $|\Psi\rangle_{AB}$  cannot be written as a tensor product of two separate states, i.e. as  $|\psi\rangle_A \times |\phi\rangle_B$ . We then say that both particles are entangled. A basic example is  $(|0\rangle_A \times |1\rangle_B - |1\rangle_A \times |0\rangle_B)/\sqrt{2}$ .

It has been shown that entangled photons can enhance the spatial resolution of imaging beyond the classical diffraction limit [56, 57]. 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  $N$ ) [57]. More specifically, considering the Airy disk mentioned before, we can reduce its radius to

$$\xi_{quantum} = 0.61\lambda LRN$$

using  $N+1$  entangled photons, which is  $N$  times smaller than the classical case and this, hence, presents a sub-Rayleigh resolution. The way this is done is by sending  $N$  degenerate photons to the object, keep the non-degenerate photon 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.

### E.3.2 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 (E.7)). Two important squeezed states are the phase-squeezed light and amplitude-squeezed light, which have decreased uncertainty in the electromagnetic wave's phase 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.

## E.4 Applications

As mentioned before, the straightforward 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, differently from 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

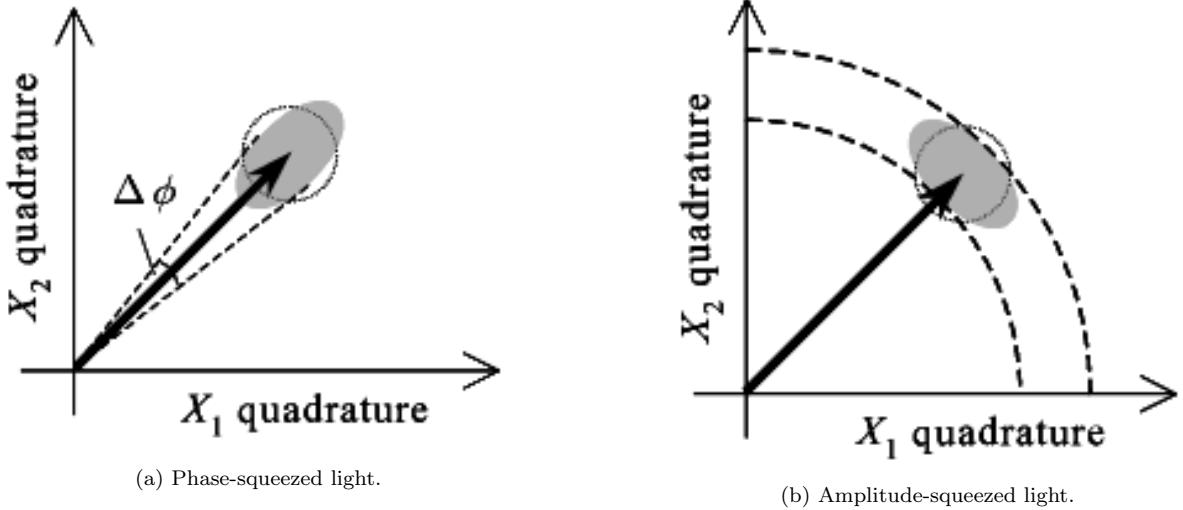


Figure E.7: Quadrature squeezed states. The dotted circle in each of the diagrams shows the quadrature uncertainty of the states with  $\Delta X_1 = \Delta X_2 = 1/2$ . Taken from [1].

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 photo spatial resolution and improving its quality.

On one hand, one of the greatest challenges to be overcome in order to achieve this technology is the entanglement itself. Entangling photons is extremely hard, specially if  $N$  is large. The current record for photons entanglement is 10 photons [58]. 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 [59, 60]. 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 has been some experiments which achieved one-million-mode continuous-variable cluster states [61, 62], it is still necessary to ascertain if this kind of states 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 [63], having then already found some applications, e.g. in medical areas and biology, interferometric measurements with gravitational waves [64], spectroscopic signals [65] and atomic clocks [66]. Regarding biology, it was already used to image a living cell [67] and to study proteins [68]. However being easier, it does not present the same improvement over sensitivity than the use of entangled photons does.

## F Quantum Enhanced Solar Cells

Inefficiencies in the energy storage 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 [69], 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 [2]. Moreover, green light has shown no regulatory benefit in this scheme, and therefore should not be absorbed by the photocell in the optimal case. Interestingly, energy fluctuations can lead to similar inefficiencies in photosynthesis due to oxidative damage. Consequently, it is possible that a similar quantum thermodynamic mechanism to that of the quantum photocell occurs in photosynthesis, resulting in the low absorption of green light in plants.

### F.1 Comparison to Current Techniques

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 [70]. 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 [71, 72]. Classical solar technology also utilises semiconductor material linked by a bandgap such that individual photons are absorbed, producing photoelectrons [73]. 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 [69]. 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 [2].

### F.2 The Quantum Enhanced Photocell

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 [2].

In order to describe the power transfer and fluctuations of such a two channel photocell proposed in [2], 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  $\gamma_a$  and  $\gamma_b$ , 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  $\Gamma$  causing them to decay to a low energy state  $|y\rangle$  and eventually the ground state  $|g\rangle$  at a rate  $\gamma_g$ . This process is illustrated in Fig. F.8.

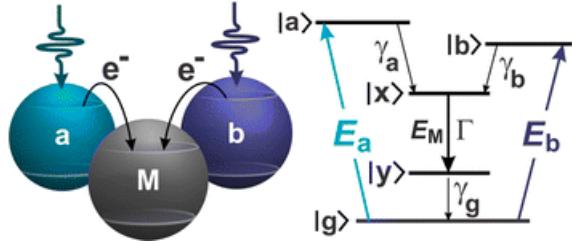


Figure F.8: (Left) Schematic of a two-channel quantum photocell. Photons absorbed by channel  $a$  and  $b$  give rise to a pair of photoelectrons, generating electronic power in the machine  $M$ . (Right) Energy level diagram of the two-channel quantum photocell.  $E_a$  and  $E_b$  are the excitation energies of the channels  $a$  and  $b$  with transition rates to the machine  $M$  given by  $\gamma_a$  and  $\gamma_b$  respectively. The output energy is given by  $E_M$  and is characterised by the rate of relaxation  $\Gamma$  from state  $|x\rangle$  to state  $|y\rangle$ .  $\gamma_g$  represents the rate of decay to the ground state  $|g\rangle$  [2].

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  $\sigma^2 = p_a(u_a - u_M)^2 + p_b(u_b - u_M)^2 + (1 - p_a - p_b)u_M^2$  from the definition  $Var(x) = \sum_i [p_i(x_i - \mu)^2]$ . 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  $\lambda$  and temperature

$T$  to be described by an irradiance spectrum  $I(\lambda, T)$ , the average input energy flux can be written as  $u_i = \int A_i(\lambda)I(\lambda, T)d\lambda$ , 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, in order 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  $u_b$ . Also, it has been 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. Semiconductor nanostructures have been shown to be promising candidates for light harvesting independently of this research, as they have remarkably high absorption, a high efficiency of charge transfer and an intrinsically high power conversion efficiency [74]. It is possible to engineer quantum dots with these properties [75], and by electronic coupling of quantum dots the increased power conversion efficiency as a result of these features and two-channel absorption could be directly observable.

### F.3 Nature-inspired Quantum Alternatives

Despite the promising design for a quantum photocell described here, there also exist more biology-inspired suggestions for organic photovoltaics devices which take advantage of quantum coherence effects similar to those observed in biological photosynthetic systems [76, 77]. Such systems would use materials which enable a more delocalized 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.

## G Quantum Enhanced Material Detection

## H 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, year 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 through 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 [78]. 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 gas-powered vehicles [79].

### H.1 Classical

Despite the battery industry has moved between materials and technology schemes along 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 some 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. Provided a quantum heat engine that 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 [80]) which allows extraction of work from one thermal bath. If one has a d-level system in a pure state  $\psi$  one can draw  $kT\ln(d)$  work out of heat bath of temperature T. If a state of the system is a mixed state  $\rho$ , then the amount of work would correspond to

$$W = kT\ln(d) - TS(\rho) \quad (1)$$

where  $S(\rho) = ks(\rho)$ ;  $s(\rho)$  is von Neumann entropy and  $k$  is the Boltzmann constant [81]. The equivalence between work and information opened a new way of thinking about the thermodynamics of quantum systems.

## H.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 center. 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  $\rho$  and the internal Hamiltonian  $H$  [82]. This quantity called ergotropy is given by

$$W_{max} = \text{tr}(\rho H) - \min [\text{tr}(U \rho U^\dagger H)], \quad (2)$$

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

$$U(\tau) = \exp \left( -i \int_0^\tau ds [H + V(s)] \right). \quad (3)$$

This unitary transformation determines the evolution of the system. Note that by a proper choice of the field  $V(t)$  any unitary  $U$  can be obtained. The minimum in equation (2) 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. Allicky and Fannes showed that the extractable work can be increased by allowing entangling operations [83].

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 [3] and bounds for an achievable quantum advantage using entanglement in multi-partite systems have been found [84].

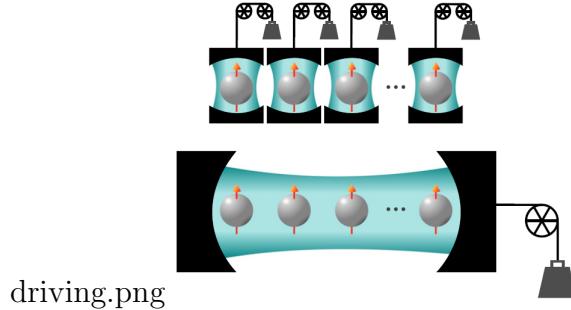


Figure H.9: An array of qubits that represent a quantum battery. They can either be driven in parallel or globally to extract work from them or charge them. This image is taken from [3] where they showed that the correlations between the qubits affect the charging power when the system is drove globally.

### H.3 Discussion

Although many of this results on 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 scientist 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 interval of time allowing us to have control on the quantum state of say, the reactants inside the batteries providing us a new generation of batteries.

# I 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 microgal per hertz<sup>1/2</sup> are required.

To get an understanding of scale,  $1 \text{ gal} = 1 \text{ cm/s}^2 = 0.01 \text{ m/s}^2$ , roughly 4 orders of magnitude less than acceleration due to gravity experienced by a mass at the Earth's surface. A microgal is therefore 10 orders of magnitude less than this. The gravity gradient (variation with height) above Earth's surface is about  $3.1 \mu \text{ Gal}$  per centimeter of height ( $3.1 \times 10^{-6} \text{ s}^{-2}$ ) and one gal hertz<sup>1/2</sup> is a measurement of 1 gal over an integration time of one second, the variance of the acceleration from a value.

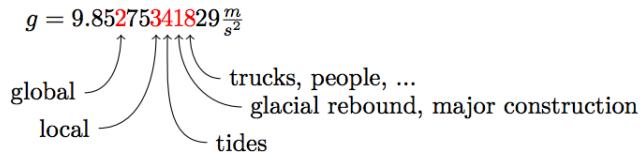


Figure I.10: An indication of the precision required to detect the acceleration due to gravity relative to that of the planet. Figure taken from [85]

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 microgal per hertz<sup>1/2</sup> [86]. 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 relative gravimeter still costs over \$100,000, has a precision of 2 microgal per hertz<sup>1/2</sup>, is only 8 kg but is susceptible to drift, that is, the change in time of the measured data in unpredictable ways [87].

Gravity sensing applications are centered 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 measurements, 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 object 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 is 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 measurement 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  $\text{ms}^{-2}$  at the equator [88].

Object	Mass/kg	Distance/m	Gravity/ $\mu\text{Gal}$	Gradient/ $\mu\text{Gal m}^{-1}$	Angle/degree	Gravity change/ $\mu\text{Gal}$
Earth	$6.0 \times 10^{24}$	$6.4 \times 10^6$	$9.8 \times 10^8$	308	0	$9.8 \times 10^8$
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)	$2.0 \times 10^6$	50	5.0	0.2	90	0.0
Hole (excavated)	$2.0 \times 10^7$	100	13.3	0.3	85	1.3

Figure I.11: Absolute examples of the acceleration of various objects. Figure taken from [89]

## I.1 Classical

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

### I.1.1 Spring

One example of a classical gravity sensor that is one 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 now have a sensitivity of 40 microgal per hertz $^{1/2}$  [90], that is, changes corresponding to a change in height from the Earth's surface of around 600 meters can be distinguished from noise or a change in mass at equal distance of  $2 \times 10^{17}$

(roughly  $1 \mu \%$  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 the the extension of the spring is dependent on the gravity at any point in time.

### I.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 one nanogal, one thousandth of one billionth ( $10^{-12}$ ) of the Earth surface gravity.

### I.1.3 Free-fall

The motion of a free falling corner-cube retroreflector in vacuum is monitored by a laser interferometer, see Fig I.12, 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.

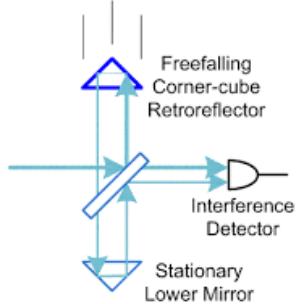


Figure I.12: Image taken from [91]

## I.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 recombined to produce interference fringes, see Fig I.13. Light pulse 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.

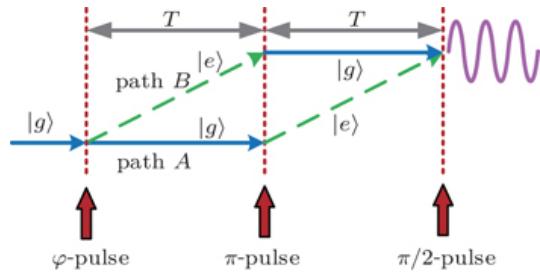


Figure I.13: Time period  $T$  between pulses, where  $|g\rangle$  and  $|e\rangle$  represent the two occupied states of the system. Image taken from [92]

The process of atomic interferometry is more precisely described below and is described in more detail by Hauth *et al* [93].

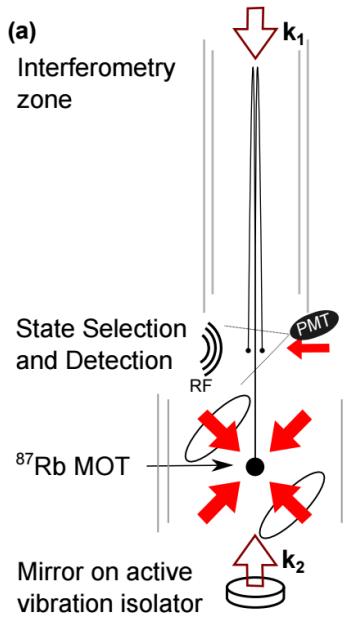


Figure I.14:  $k_1$  and  $k_2$  are the wavevectors of Rabi pulses. Image taken from [94]

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  $\mu\text{K}$ . The cloud is launched upwards using far-detuned optical molasses (a 3-D 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 atom is excited to virtual energy level by off-resonant light and then deexcited 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 [95]. Further, 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, where the atoms are fed through a conceptual Mach-Zehnder interferometer. A  $\pi$ -pulse in this analogy acts as a mirror and a  $\pi/2$ -pulse as a beamsplitter, Fig I.13. 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  $\pi$ -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.

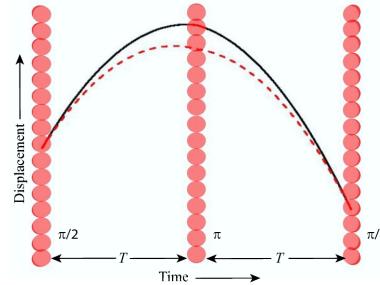


Figure I.15: Image taken from [96]

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

$$P_{F_2} = \bar{P} + \frac{C}{2} \cos \Delta\phi \quad (4)$$

$C$  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

$$\Delta\phi = (k_{\text{eff}}g = \alpha) \cdot T^2 + \Delta\phi_L \quad (5)$$

where  $k_{\text{eff}}$  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.  $\alpha$  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  $\alpha$  and  $\Delta\phi_L$  until the phase difference is zero and hence the population of the  $F = 2$  state is maximal.

### I.2.1 Examples: 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  $1 \times 10^{-12}$  [97], which will impose new limits on the violation scenarios of the universality of free fall.

Further, Bose Einstein Condensate (BEC)s promise to increase the accuracy of quantum gravity sensing below the  $\mu\text{Gal}$  limit [98] [99]. 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 millimeters, shows promise to extend the accuracy of robust and compact gravimeters sensitive to a variations of a few  $\mu\text{Gal}$  and accurate to sub- $\mu\text{Gal}$  levels in an optimised setup.

## I.3 Discussion

The greatest advantage of Quantum Gravity Sensors (QGS) 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, defense 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 system 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 [100].

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. 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 fulfill 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. Further, 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.

## J Quantum Magnetic Sensors

### J.1 Introduction

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) [101, 102]. Electroencephalography (EEG) is an alternative to MEG, and uses electrodes to sense changes in bioelectric fields to monitor the same biological processes as MEG [103]. 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.

### J.2 The Current Technology

To date, systems used for measuring biomagnetic fields such as MEG and MRI scanners have relied on SQUIDS, which exploit quantum effects in superconducting loops containing two Josephson Junctions [104]. 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  $I_s$  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  $\phi_0$  since the flux in the superconducting loop is quantised by integer multiples of  $\phi_0$ . Therefore, the screening current flows in the opposite direction, and this happens periodically, giving rise to oscillatory current with a period of  $\phi_0$ . 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 [105]. EEG measurements are used to record the electrical activity in a subjects brain, and requires a simpler apparatus than MEG and MRI [106]. In this procedure, a direct measurement of electric fields is performed by placing an array of electrodes on the subjects head, before amplifying and filtering the electrical output to monitor neural activity.

### J.3 Quantum Enhanced Magnetic Sensing

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 [4, 107–112]. 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 magnetization 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 [113]. It is possible to create very compact magnetometers using this technique, and Fig. J.16 shows a design for a microfabricated optical magnetometer which demonstrated very high sensitivities.

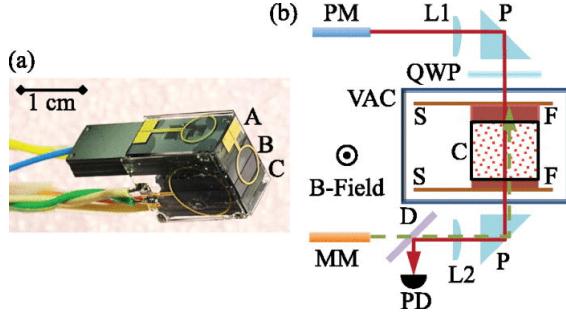


Figure J.16: (a) Photograph of the microfabricated optical magnetometer sensor in [4]. The size of the sensor head is approximately 0.36cm. The fibre for the probe beam is held in structure A, the atomic vapour cell in structure B, and the photodetector and heating light fibre in structure C. (b) Diagram 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.

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 [5, 114–116]. The experimental setup for the QND magnetometer in [5] is shown in Fig. J.17. In these measurement schemes, a pump beam is used to spin-polarize 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.

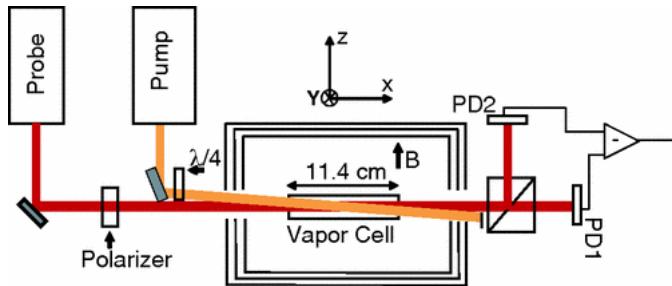


Figure J.17: Diagram of the experimental apparatus for a typical QND atomic magnetometer as in [5]. A pump laser is used to spin polarize the atomic vapour, and a linearly polarized probe beam is directed along the length of the cell. Paramagnetic Faraday rotation induced by the atoms is measured with a balanced polarimeter, from which the magnetic field can be derived.

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 [117], 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. Other atomic magnetometry experiments have instead used squeezed light sources to probe the vapour of atomic spins [118, 119], 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 [120].

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 [121]. 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 [122]. 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 [6, 7, 123–125]. 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 Fig. J.18.

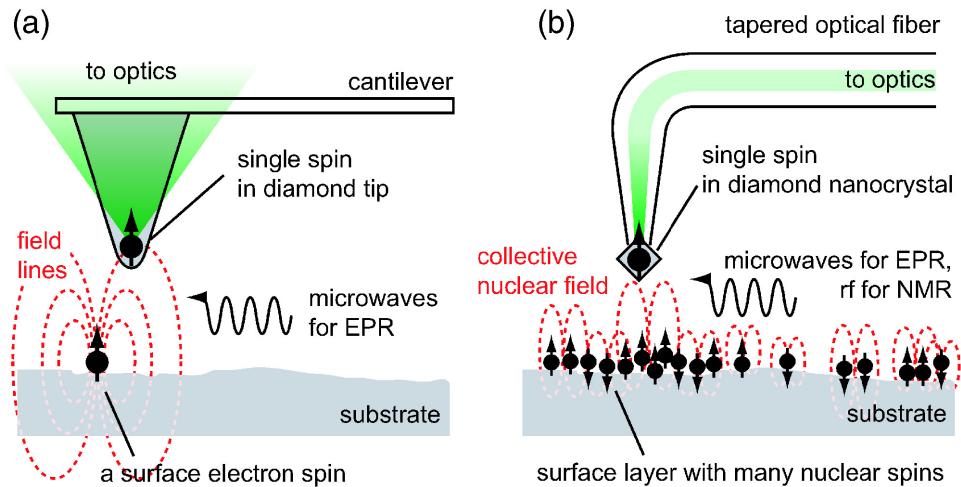


Figure J.18: Schematic of the diamond-based scanning spin microscope in [6]. Changes in the local magnetic fields will result in a shift of the electron spin resonance (EPR) frequency, and these magnetic fields can be measured by monitoring the corresponding change in photoluminescence of the probe spin. In (a), a single electron spin in an NV centre on the tip of an 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.

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 sensing the magnetic field emitted by remote objects, such as a human heart or brain. Fig. J.19 illustrates an example of how this may be achieved, by measuring the photoluminescence from a larger sample of diamond.

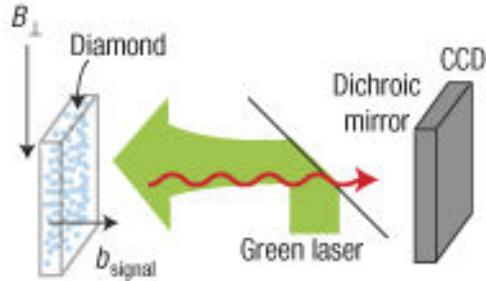


Figure J.19: This schematic illustrates a bulk diamond magnetometer with a high density of NV centres for sensing fields created by remote objects, as proposed in [7]. Here, a laser beam directed onto the sample induces spin-dependent photoluminescence, which can be detected using a CCD.

It can be shown that with an NV centre consisting of a single electron spin, the fluctuations in the detuning  $\omega$  due to the Zeeman splitting induced by the target magnetic field are bounded by  $|\delta\omega| \approx 1/\alpha\sqrt{MT_{2e}^*}$  [126], where  $\alpha$  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 [126]. 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 [127].

## J.4 Applications

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 [128–130], as this is the only sensor capable of measuring the magnetic field of a persons 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 [131, 132], 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.

## K 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. An entity of interest is targeted through the choice of chemicals used to coat the fluorophore, which determines what it will repel, attract or bond to. The sample is then irradiated with 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 [133].

### K.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 [133]. Fluorescent proteins go a step further; by adding a fluorescent protein sequence to the target-protein sequence in the organism 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' [134], 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 [135].

### K.2 Quantum

In 1998, a new type of fluorophore was proposed - the quantum dot (QD) [136,137]. Quantum dots have proved much more resistant to photobleaching, and are brighter than the alternatives, giving higher quality images [138,139]. 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 [140].

A quantum dot is a nano-scale 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 K.20. 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.

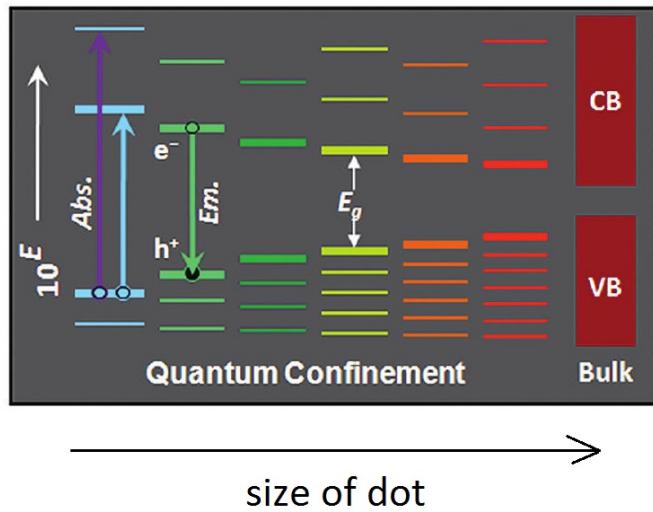


Figure K.20: Diagram illustrating the correlation between the diameter of the quantum dot and the size of the semiconductor bandgap. Colours indicate the larger dots produce light towards the red end of the spectrum as the electron transition across the bandgap is smaller. The purple arrow illustrates excitation across the bandgap by the UV source. Image taken from [138]

### K.3 Discussion

Fluorescence microscopy has matured to commercial devices, which are enabling much more rapid medical diagnosis than the traditional method of culturing the sample [133], i.e. waiting several hours for the pathogens to populate a nutrient medium for detection by eye. It may even be possible to miniaturise and automate the process to enable biosensors, by scanning the sample for points of high light intensity, indicating

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 dot has a CdSe core with a ZnS shell, simply due to ease of fabrication by the hot-injection method [138]. 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 coated with branched poly-ethylenimine, [poly1, poly2] which were used to detect Cu<sup>2+</sup> ions. The Cu<sup>2+</sup> ions

reduced the fluorescence of the dots when attached to them (referred to as quenching), allowing measurement of the Cu<sup>2+</sup> concentration [poly2].

Using the same principle of fluorescence quenching, a system for detection and differentiation of explosives using QDs was tested [141]. As illustrated in figure K.21, 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.

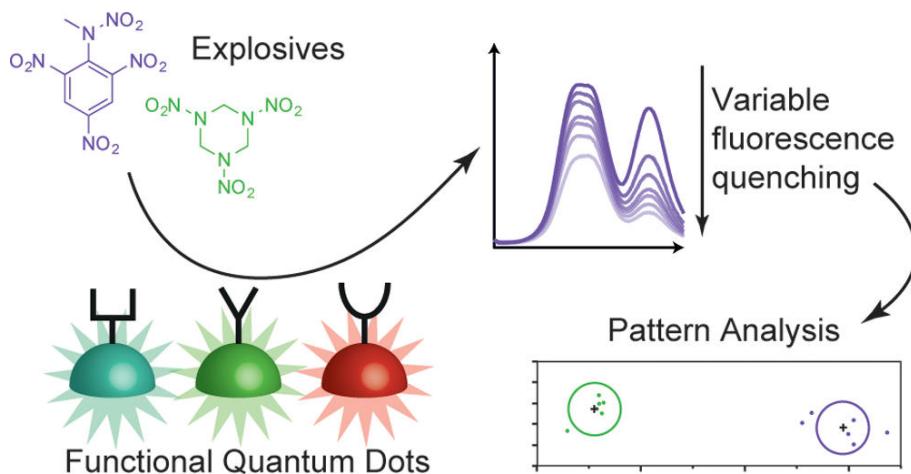


Figure K.21: Illustration of the quantum dot explosives detection scheme from [141].

Using QDs in conjunction with super-resolution microscopy techniques such as SNOM (scanning near-field optical microscopy) or STED (stimulated emission depletion) enables . . . single molecule detection? another property of quantum dots - blinking comes in handy here [2015 review p4797]. QDs fluorescence turns on and off intermittently, with no characteristic recovery time, so coincidental blinking is rare, which allows resolution of individual dots.

Properties other than fluorescence of QDs can be used to obtain additional information. An alternative proposition exploits ‘photoinduced charge carrier transfer’ [142], 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 [143] 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) [144].

# L Quantum Money

## L.1 Introduction

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. By the time of this writing, a single Bitcoin, whose value was less than \$0.003 in 2010, equals around \$4000.

Both these approaches to money have problems, or at least can have in the future. Paper money (unlike gold, silver or the cryptocurrencies) can be frauded 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 threat their system. We shall then explore in which ways the quantum technologies might solve these problems.

## L.2 Classical

In the following we briefly review the current (classical) versions of both paper money and cryptocurrencies, paying more attention to the last since it might be new to some people.

### L.2.1 Paper Money

As mentioned before, 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 wishes that money has 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, specially scarcity, can escape our attention, since paper money does not have these characteristics. We desire irreplicability as a condition to avoid counterfeit by general people. On the other hand, governments usually print money as one of their principal economic polities. Fiat money needs then to be easy to be printed by central banks but hard to be forged by others. Therefore governments spend put a substantial effort in developing anti-counterfeiting measures. Traditionally, these measures involve including fine detail with raised intaglio printing on bills 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 L.22 shows anti-counterfeiting features on an U.S. \$20 bill.

One also wants to 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 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.

### L.2.2 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.<sup>1</sup>

There are several cryptographic technologies that make up the essence of Bitcoin [145]. 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 to the owner. This

---

<sup>1</sup><https://www.coingecko.com>

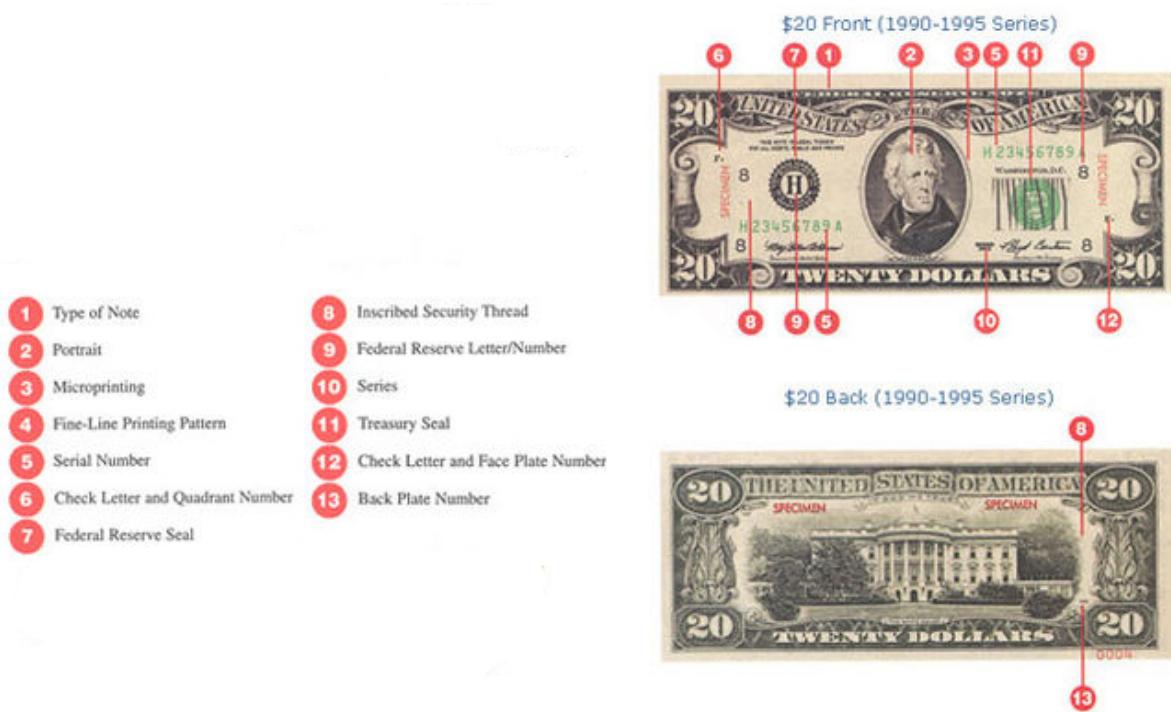


Figure L.22: Anti-counterfeiting features on an old U.S. \$20 bill.

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 [146, 147]. 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 (L.23)). 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.

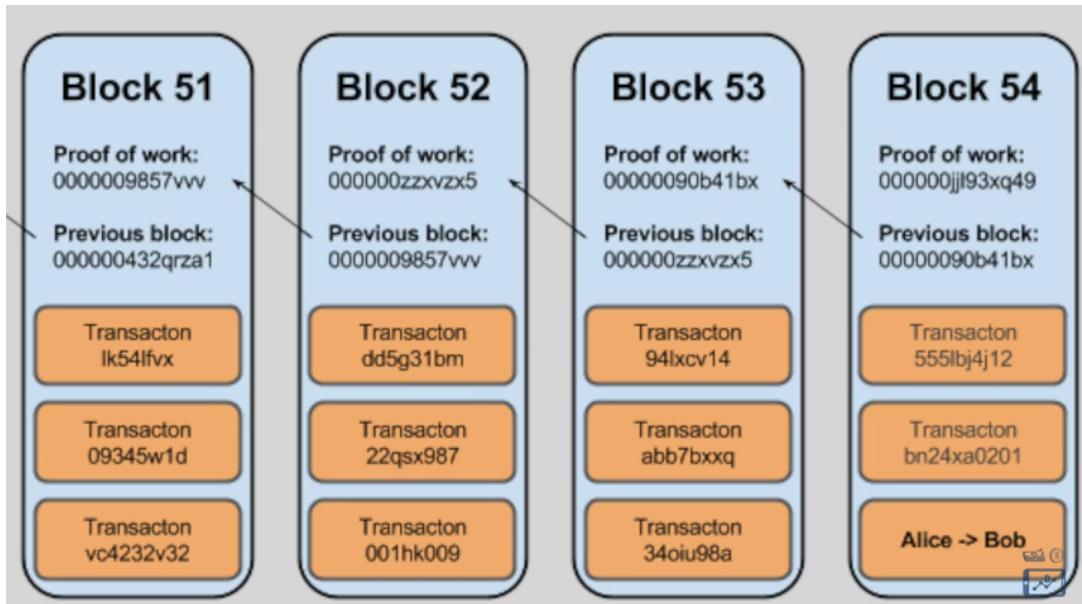


Figure L.23: The block chain and some of its blocks. Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block.

To make generating bitcoins difficult the Hashcash cost-function is used [148]. 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) [149, 150].

The block chain and the public key cryptography are the main part 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.

## L.3 Quantum

Both banknotes and cryptocurrencies might benefit from the 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.

### L.3.1 Paper Money

The idea of a proposed design of bank notes which makes them impossible to forge with the use of quantum mechanics was put forward in about 1970 by Stephen Wiesner [151]. 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 bill in a quantum state, it is not possible to duplicate the bill.

Wiesner used the photons as a system for encoding information. In each bill, there is a sequence of quantum states in one of two complementary bases. For example, photons in one of four polarizations 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 polarizations 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 polarizations of these states cannot copy them.

In addition to actual physical system, there would be a unique serial number on each bank note, which corresponds to note's set of polarizations 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 polarizations by measuring the polarization 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 polarization states, since even if he knows the two bases, if he chooses the wrong one to measure a photon, it will change the polarization of the photon in the trap, and the forged banknote created will be with this wrong polarization. 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.

# M Quantum Pattern Matching

NOT FINISHED!

## M.1 Introduction

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 [152–154].

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 upto 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 adiabatic quantum computers could be a way forward.

## M.2 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 be 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 remember 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.

First, we look at dimensionality reduction. The algorithm must determine 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 [155]. However, the most common algorithms are principal component analysis [156] and linear discriminant analysis [157], which are both holistic. Other notable algorithms are vector quantisation [158], which is also holistic and non-negative matrix factorisation [159], which is feature-based.

All these algorithms aim to represent a face as a linear combination of basis elements. Equivalently, it can be formulated as a matrix  $V = WH$ , 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  $H$  [160].  $Wh$  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  $i$ th element in vector  $h$ , and  $W_i$  is the  $i$ th 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 something, 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). 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. This minimisation is an optimisation problem which is predominantly performed using 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 the training phase 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 unlabeled training data such that it is not classed as correct or incorrect. In supervised algorithms, the data used is labeled and so the desired output is known. Supervised algorithms maximise the class discrimination and unsupervised algorithms minimise the information loss.

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. 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. PCA is an unsupervised algorithm as it minimises variation loss as it ignores vectors that contain the least variation in data and the data is unlabeled.

LDA maximises the distance between classes - ie. wants data to give big differences between different faces and small differences for images of the same face. It is a supervised algorithm as it maximises the class discrimination and uses labeled data (the input faces are known whether they are the same or not).

Comparison of NMF and PCA and different metrics and under different conditions [161].

Neural networks LVQ [158]

### M.3 Quantum

Quantum machine learning [162, 163]. Firstly, an algorithm for quantum principal component analysis has been proposed [164], which has an exponential speed up over the classical case.

Quantum machine learning is a recent field emerging from the inclusion of quantum principles in machine learning. Universal quantum computers are yet to be demonstrated, but D-wave have demonstrated quantum supremacy using their adiabatic quantum annealers. They have proposed a method that uses their quantum annealers for matrix factorisation [165]. This method, non-negative/binary matrix factorisation (NBMF), 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,

$$W = \arg(\min_{X \in R^{n \times k}} X - VH_F + \alpha X_F); \quad (6)$$

$$H = \arg(\min_{X \in \{0,1\}^{k \times m}} V - WX_F); \quad (7)$$

end while;

#### 4. Output $W$ and $H$ .

Here, we will focus on solving equation 7. 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  $i$ th column of  $V - WX$  only depends on the  $i$ th column of  $V$  and  $X$ . Hence we can equation 7 with  $km$  binary variables to  $m$  optimisation problems with  $k$  binary variables each:

$$H_i = \arg(\min_{X \in \{0,1\}^k} V_i - WX_{i2}), \quad (8)$$

where  $H_i$ ,  $V_i$  and  $X_i$  denote the  $i$ th 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 [165].

## M.4 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 this 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.

Pattern matching is an NP-hard problem which is classically intractable and so approximations are made to solve it classically. Quantum computers would be able to solve the problem exactly which could result in a more accurate answer.

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 [166]. 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. The dimensionality reduction is similar

in that it tries to remove any words that commonly occur in all emails and keeps only the parts useful for determining the difference between spam and not spam, for example.

## N Superman Memory Crystal

## O Quantum Teleportation

# P 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.

## P.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 EMV standards for chip cards and contactless cards [167]). 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 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 Numbers (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 [168, 169]. 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 [170], with the potential to cause a continual battle between fraud and banks.

One way to help improve security would be to use a QRNG [171], such as in appendix B, 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 [172] 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 [173] such as a man-in-the-middle attack, which has the potential to read these numbers and use them, pretending to be the consumer.

## P.2 Quantum

To get around this potential flaw, the ideas of QKD are used: instead of transmitting a series of bits, the first QKD protocols, such as BB84, use a series of photons that are polarisation encoded by a random number 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

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	D	R	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	0	1	1	1	1	1	0	0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits .....	R	D	R	D	D	R	R	D	D	D	D	D	D	D	R
Alice says which bases were correct .....	OK														
Presumably shared information (if no eavesdrop)	1	1	1	0	0	0	0	1	0	1	0	0	0	0	1
Bob reveals some key bits at random .....															0
Alice confirms them .....															OK
OUTCOME															
Remaining shared secret bits .....	1								0				1		1

Figure P.24: 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 [11]

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 Q.30 [11]. 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 [174, 175].

## P.3 Discussion

### P.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 Light Emitting Diodes (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 P.25, then into a receiver and measured [8] as shown in figure P.26. This technology already exists and is shown in figure P.27. 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 Q, could potentially be used to send the single photons through a fibre through a network to the bank.



Figure P.25: 4 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 [8]

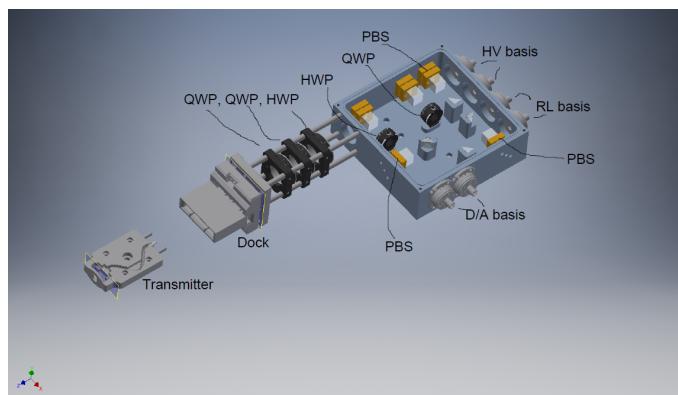


Figure P.26: Schematic of the receiving device used to perform handheld QKD. Image provided by David Lowndes

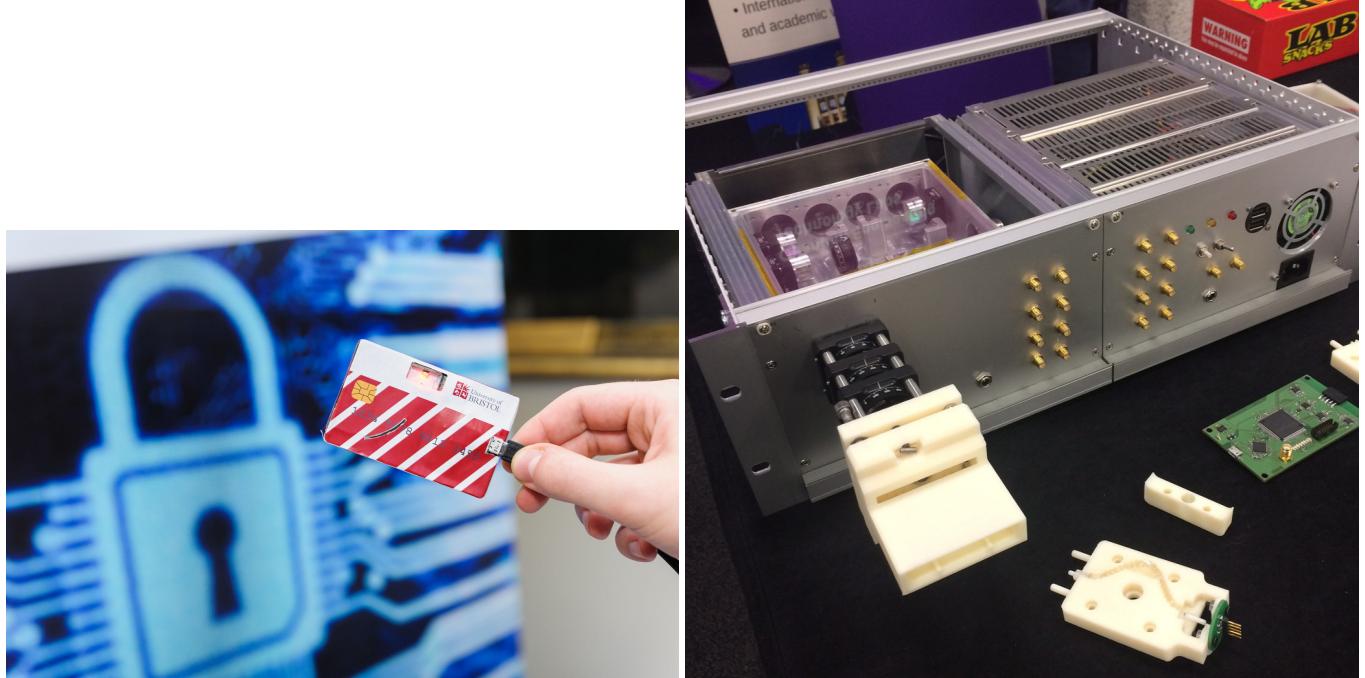


Figure P.27: Photos of the transmitting (left) and receiving (right) devices used to perform handheld QKD. Image provided by David Lowndes

### **P.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 [176] 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.

### **P.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’ or only able to be copied by the receiver that knows the bases of the measurement (which can be decided by another random number).

# **Q 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 [177], Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) [178, 179], 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 Quantum Key Distribution. Quantum technology also allows for improved methods of data transfer, such as using increased speeds or quantum teleportation.

## **Q.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 Q.28. 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 IEEE 802.3: Ethernet standard [179], 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 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) [180–182], 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 ISO/IEC FDIS 11801 standard [183].

## **Q.2 Quantum**

The ability to send a quantum signal 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 [184–186], quantum

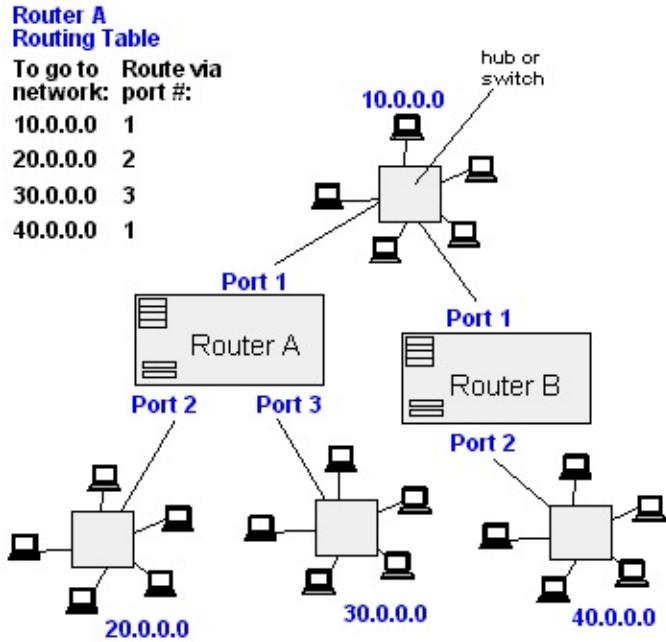


Figure Q.28: Route forwarding protocol. Packets containing the final IP address are sent through a port to a router, which decides which port to transmit the packet along based on the IP address in the header of the packet. This process repeats until the data reaches its final destination. Image taken from [9]

state teleportation (described in appendix O), authentication (as, for example, in appendix P) and blind quantum computing, explained below. 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 [187], over a few hundred km to a fixed receiver [188] or even to satellites [189, 190]

## Q.3 Discussion

### Q.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 [191], or using satellites, such as in [189, 190, 192].

However, the other issues are more problematic. The first is that loss in fibre at  $0.1\text{--}0.2 \text{ dB km}^{-1}$  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 [10, 193], where one photon

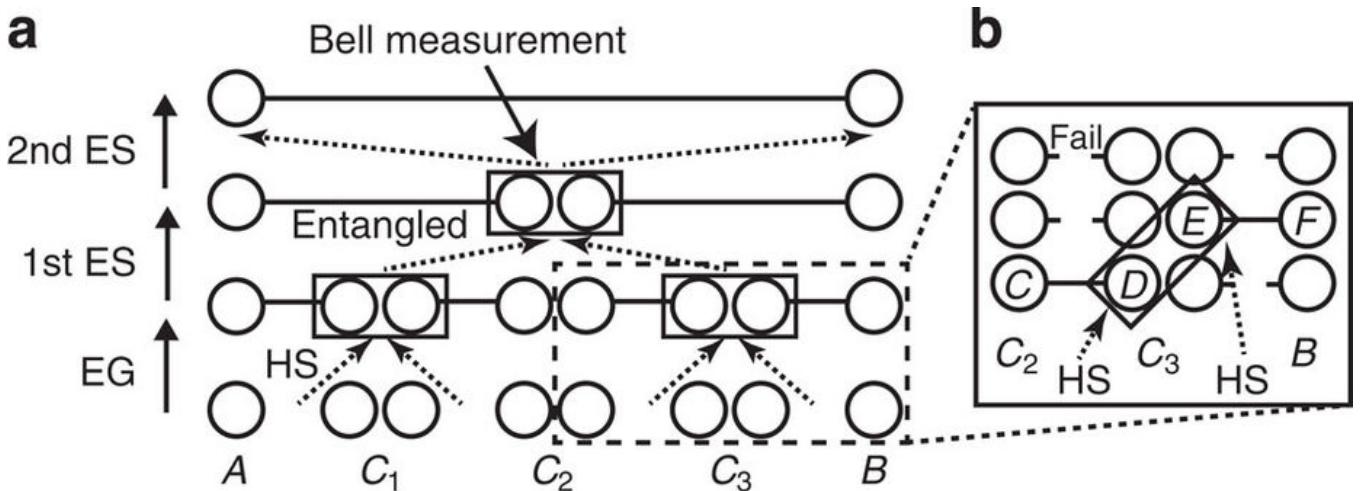


Figure Q.29: a) basic repeater protocol involving creating entangled pairs of signal and idler photons (Entanglement Generation, EG) between neighbouring nodes and recursively calling the Entanglement Swapping (ES) operation where the photons of a node are heralded (heralding signal, HS) in order to 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 [10]

from each of two pairs of entangles photons is put through a beam splitter and measured, as in figure Q.29; 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; or potentially satellites before single photons can be sent over long distances. 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 Q.28 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 £100k per box [194, 195]. This is sufficient for quantum key distribution, which allows for secure data transmission between A and B. A cheaper method than this would be to use LEDs, as in appendix P.

### Q.3.2 Quantum Key Distribution

As explained in appendix P, the first QKD protocols, such as BB84, were a series of photons that are polarisation encoded by a random number 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

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	D	R	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	0	0	1	1	1	1	0	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 Q.30: Basic Idea of the BB84 QKD 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 [11]

sender and receiver and receiving a percentage of incorrect polarisations above a threshold value after the protocol indicates an eavesdropper as shown in figure Q.30 [11]. 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 [174, 175]. Many current commercially available methods of QKD involve protocols such as Coherent One Way (COW) [195, 196] and SARG [194, 197], which work using attenuated lasers with an average number of photons,  $\mu < 1$  and encoding the qubits using orthogonal bases.

Current rates for quantum key distribution are 10Gbps (which would be the same as possible using the states as the above paragraph for non-secure data transmission using forward error correction, more than an order of magnitude greater than currently possible). Over 50km, this reduces to 1Mbps 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 [198] by an amount depending on the number of channels used, possibly by at least another order of magnitude.

### Q.3.3 Blind Quantum Computing

write

# R 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 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 quantum level is known to be impossible for classical computers since the resources required scale exponentially with the system size [23].

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.” [199]. 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 exponential amount of information without taking up exponential amount of physical resources. Different techniques of manipulating them could lead to the next generation of computer simulators.

## R.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.

### R.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 [200].

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 [201].

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 [202]. However, most of them suffer from similar to Monte Carlo methods' problems which ultimately prevents them from successfully simulating quantum physics.

## R.2 Quantum

Quantum simulator is a controllable quantum system which is used to emulate another quantum systems [203]. Schematics of how this works can be seen in fig. Depending on the level of control and capabilities of the simulator there are two types of simulation, analog and digital.

### R.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 [204]:

$$\begin{aligned} f : H_{sys} &\rightarrow H_{sim} \\ f^{-1} : H_{sim} &\rightarrow H_{sys} \end{aligned}$$

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 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.

### R.2.2 Digital Quantum Simulations

In digital quantum computing Digital Quantum Simulation (DQS), all information is encoded using superposition 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  $|1\rangle$ . 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 [205]. An example of how this scheme works can be seen in Fig.

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 [206]. 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 used to simulate almost any real system as soon as a universal quantum computer is build.

## Applications

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.

### R.2.3 Electronics

Learning more about fundamental physics phenomena can help shedding 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 AQS is the  $t$ - $J$  model which describes strongly correlated fermions on a lattice [207]. 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 [208].

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 [209]. Developing these systems would allow precise control over the propagation of electromagnetic fields unachievable by standard materials.

#### R.2.4 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 initialized to contain 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 [210].

## References

- [1] M. Fox. *Quantum Optics: An Introduction*. Oxford Master Series in Physics. OUP Oxford, 2006.
- [2] 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.
- [3] Felix C Binder, Sai Vinjanampathy, Kavan Modi, and John Goold. Quantacell: powerful charging of quantum batteries. *New Journal of Physics*, 17(7):075015, 2015.
- [4] R Mhaskar, S Knappe, and J Kitching. A low-power, high-sensitivity micromachined optical magnetometer. *Applied Physics Letters*, 101(24):241105, 2012.
- [5] V Shah, G Vasilakis, and MV Romalis. High bandwidth atomic magnetometry with continuous quantum nondemolition measurements. *Physical review letters*, 104(1):013601, 2010.
- [6] CL Degen. Scanning magnetic field microscope with a diamond single-spin sensor. *Applied Physics Letters*, 92(24):243111, 2008.
- [7] 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.
- [8] 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.
- [9] THe Free Dictionary. Network router.
- [10] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. All-photonic quantum repeaters. *Nature communications*, 6, 2015.

- [11] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and con tos5. 1984.
- [12] Homeland Security Research. Quantum computing market & technologies - 2017-2024. *Homeland Security Research*, 2017.
- [13] 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.
- [14] White House. America first: A budget blueprint to make america great again. *March*, 16:50, 2017.
- [15] IARPA. Quantum programs at iarpa. <https://www.iarpa.gov/index.php/research-programs/quantum-programs-at-iarpa>, 2017.
- [16] HM Treasury. Autumn statement 2013. *Crown copyright*, 2013.
- [17] Qurope. Quantum manifesto: A new era of technology. *Qurope*, 2016.
- [18] Freeke Heijman te Paske. Global developments in quantum technologies. <https://connect.innovateuk.org/documents/11487824/26842605/Global+Developments+in+Quantum+Technology/>, 2015.
- [19] George Stoye. Uk health spending. 2017.
- [20] Kaare Christensen, Gabriele Doblhammer, Roland Rau, and James W Vaupel. Ageing populations: the challenges ahead. *The lancet*, 374(9696):1196–1208, 2009.
- [21] 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.
- [22] OECD. Fiscal sustainability of health systems: Bridging health and finance perspectives. *OECD*, 2015.
- [23] Richard P Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6):467–488, 1982.
- [24] 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.
- [25] 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.
- [26] 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.
- [27] Philip Sibson, Chris Erven, Mark Godfrey, Shigehito Miki, Taro Yamashita, Mikio Fujiwara, Masahide Sasaki, Hirotaka Terai, Michael G Tanner, Chandra M Natarajan, et al. Chip-based quantum key distribution. *Nature Communications*, 8:13984, 2017.

- [28] World Economic Forum. Global risks 2017. <http://reports.weforum.org/global-risks-2017/part-1-global-risks-2017/>, 2017.
- [29] 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.
- [30] IHS Technology Sam Wilkinson. Grid-connected energy storage report. 2015.
- [31] World Economic Forum. Renewable infrastructure investment handbook: A guide for institutional investors. 2016.
- [32] Bronwyn H Hall. Innovation and productivity. Technical report, National bureau of economic research, 2011.
- [33] Science and Technology Select Committee. Connected and autonomous vehicles: The future? 2017.
- [34] IBM M. Tim Jones, developer Works. Recommender systems, part 1: Introduction to approaches and algorithms. <https://www.ibm.com/developerworks/library/os-recommender1/>, 2013.
- [35] Indranil Chakrabarty, Shahzor Khan, and Vanshdeep Singh. Dynamic grover search: applications in recommendation systems and optimization problems. *Quantum Information Processing*, 16(6):153, 2017.
- [36] Manabendra Nath Bera et al. Randomness in quantum mechanics: Philosophy, physics, and technology. *arXiv:1611.02176*, 2017.
- [37] J.M. Rist. Epicurus: An introduction.
- [38] Antonio Acin. True quantum randomness, appeared in the book "is science compatible with free will?" .
- [39] Roger Colbeck and Renato Renner. A systems wave function is uniquely determined by its underlying physical state. *New Journals of Physics*, 19(013016), 2017.
- [40] John Bell. Speakable and unspeakable in quantum mechanics, chapter 16, bertlmann's socks and the nature of reality.
- [41] Mohammad H Amin, Evgeny Andriyash, Jason Rolfe, Bohdan Kulchytskyy, and Roger Melko. Quantum boltzmann machine. *arXiv preprint arXiv:1601.02036*, 2016.
- [42] Christine Vu. Research alliance builds new transistor for 5nm technology, June 2017.
- [43] David P. Rodgers. Improvements in multiprocessor system design. *SIGARCH Comput. Archit. News*, 13(3):225–231, June 1985.
- [44] S. E. Venegas-Andraca and J. L. Ball. Processing images in entangled quantum systems. *Quantum Information Processing*, 9(1):1–11, Feb 2010.
- [45] Salvador Venegas-Andraca and Sougato Bose. Storing, processing and retrieving an image using quantum mechanics. 5105, 08 2003.
- [46] Jose I. Latorre. Image compression and entanglement. *arXiv:quant-ph/0510031*, 2005.

- [47] 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.
- [48] 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.
- [49] S Caraiman. Towards quantum computer graphics. In *Proceedings of the 14th International Conference on System Theory and Control*, pages 17–19, 2010.
- [50] Marco Lanzagorta and Jeffrey K. Uhlmann. Quantum computational geometry, 2004.
- [51] Simona Caraiman and Vasile I. Manta. Image segmentation on a quantum computer. *Quantum Information Processing*, 14(5):1693–1715, May 2015.
- [52] 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.
- [53] F.J.E.K.C. Duarte. Two-laser therapy and diagnosis device, September 28 1988. EP Patent App. EP19,880,302,468.
- [54] L. Goldman. *Dye Laser Principles*. Academic Press, Boston, 1990.
- [55] I. Garcia-Moreno A. Costela and C. Gomez. *Tunable Laser Applications*. CRC Press, Boca Raton, 3rd edition, 2016.
- [56] Y. Shih. Quantum imaging. *IEEE Journal of Selected Topics in Quantum Electronics*, 13(4):1016–1030, July 2007.
- [57] 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.
- [58] 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.
- [59] 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.
- [60] 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.
- [61] 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.

- [62] 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.
- [63] Ulrik L Andersen, Tobias Gehring, Christoph Marquardt, and Gerd Leuchs. 30 years of squeezed light generation. *Physica Scripta*, 91(5):053001, 2016.
- [64] B. P. J. Abbott *et al.* Observation of gravitational waves from a binary black hole merger. *Phys. Rev. Lett.*, 116:061102, Feb 2016.
- [65] E. S. Polzik, J. Carri, and H. J. Kimble. Spectroscopy with squeezed light. *Phys. Rev. Lett.*, 68:3020–3023, May 1992.
- [66] 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.
- [67] 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.
- [68] 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.
- [69] Sohail Anwar. *Handbook of Research on Solar Energy Systems and Technologies*. IGI Global, 2012.
- [70] JE Geusic, EO Schulz-DuBios, and HED Scovil. Quantum equivalent of the carnot cycle. *Physical Review*, 156(2):343, 1967.
- [71] 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.
- [72] AP Kirk. Analysis of quantum coherent semiconductor quantum dot p- i- n junction photovoltaic cells. *Physical review letters*, 106(4):048703, 2011.
- [73] 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.
- [74] 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.
- [75] AJ Nozik. Quantum dot solar cells. *Physica E: Low-dimensional Systems and Nanostructures*, 14(1):115–120, 2002.
- [76] 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.
- [77] 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.

- [78] Smithsonian Institution. Origin of electrical power. <http://americanhistory.si.edu/powering/past/prehist.htm>, 2002.
- [79] Jeff Desjardins. Explaining the surging demand for lithium-ion batteries. <http://www.visualcapitalist.com/explaining-surging-demand-lithium-ion-batteries>, 2016.
- [80] Erwin Schrödinger. *What is life?: With mind and matter and autobiographical sketches*. Cambridge University Press, 1992.
- [81] 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.
- [82] Armen E Allahverdyan, Roger Balian, and Th M Nieuwenhuizen. Maximal work extraction from finite quantum systems. *EPL (Europhysics Letters)*, 67(4):565, 2004.
- [83] Robert Alicki and Mark Fannes. Entanglement boost for extractable work from ensembles of quantum batteries. *Physical Review E*, 87(4):042123, 2013.
- [84] 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.
- [85] Alexander Niggebaum. *Towards mobile quantum sensors for gravity surveys*. PhD thesis, University of Birmingham, 2016.
- [86] Michel Van Camp, Simon DP Williams, and Olivier Francis. Uncertainty of absolute gravity measurements. *Journal of Geophysical Research: Solid Earth*, 110(B5), 2005.
- [87] 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.
- [88] TT In. Fundamental parameters and current (2004) best estimates of the parameters of common relevance to astronomy, geodesy, and geodynamics. 2004.
- [89] Achim Peters, Keng Yeow Chung, and Steven Chu. High-precision gravity measurements using atom interferometry. *Metrologia*, 38(1):25, 2001.
- [90] 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.
- [91] Jongmin Lee. Spring gravimeters and other alternatives. <http://large.stanford.edu/courses/2007/ph210/lee1/>.
- [92] 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.
- [93] 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.

- [94] 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.
- [95] 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.
- [96] Andrew A Geraci and Andrei Derevianko. Sensitivity of atom interferometry to ultralight scalar field dark matter. *Physical review letters*, 117(26):261301, 2016.
- [97] Jonas Hartwig, Sven Abend, Christian Schubert, Dennis Schlippert, Holger Ahlers, Katherine 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.
- [98] 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.
- [99] 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 universality of free fall using cold atom interferometry. *Classical and Quantum Gravity*, 31(11):115010, 2014.
- [100] 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.
- [101] William R Hendee and Christopher J Morgan. Magnetic resonance imaging part i—physical principles. *Western Journal of Medicine*, 141(4):491, 1984.
- [102] 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.
- [103] David A Kaiser. Basic principles of quantitative eeg. *Journal of Adult Development*, 12(2-3):99–104, 2005.
- [104] 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.
- [105] Claudia D Tesche and John Clarke. Dc squid: noise and optimization. *Journal of Low Temperature Physics*, 29(3):301–331, 1977.
- [106] Ernst Niedermeyer and FH Lopes da Silva. *Electroencephalography: basic principles, clinical applications, and related fields*. Lippincott Williams & Wilkins, 2005.

- [107] 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.
- [108] 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.
- [109] Dmitry Budker and MV Romalis. Optical magnetometry. *arXiv preprint physics/0611246*, 2006.
- [110] H Xia, A Ben-Amar Baranga, D Hoffman, and MV Romalis. Magnetoencephalography with an atomic magnetometer. *Applied Physics Letters*, 89(21):211104, 2006.
- [111] Cort N Johnson, PDD Schwindt, and M Weisend. Multi-sensor magnetoencephalography with atomic magnetometers. *Physics in medicine and biology*, 58(17):6065, 2013.
- [112] 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.
- [113] 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.
- [114] IK Kominis. Sub-shot-noise magnetometry with a correlated spin-relaxation dominated alkali-metal vapor. *Physical review letters*, 100(7):073002, 2008.
- [115] M Koschorreck, M Napolitano, B Dubost, and MW Mitchell. Sub-projection-noise sensitivity in broadband atomic magnetometry. *Physical review letters*, 104(9):093602, 2010.
- [116] 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.
- [117] D Sheng, S Li, N Dural, and MV Romalis. Subfemtesla scalar atomic magnetometry using multipass cells. *Physical review letters*, 110(16):160802, 2013.
- [118] Travis Horrom, Robinjeet Singh, Jonathan P Dowling, and Eugeni E Mikhailov. Quantum-enhanced magnetometer with low-frequency squeezing. *Physical Review A*, 86(2):023803, 2012.
- [119] 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.
- [120] Michael A Taylor and Warwick P Bowen. Quantum metrology and its application in biology. *Physics Reports*, 615:1–59, 2016.
- [121] 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.

- [122] 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.
- [123] 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.
- [124] 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.
- [125] 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.
- [126] 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.
- [127] 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.
- [128] Kazuo Tanaka, Kazuyuki Matsunaga, and Hua O Wang. Electroencephalogram-based control of an electric wheelchair. *IEEE transactions on robotics*, 21(4):762–766, 2005.
- [129] 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.
- [130] 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.
- [131] 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.
- [132] 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.
- [133] 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.
- [134] Jean Livet, Tammy 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.

- [135] 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.
- [136] Warren CW Chan and Shuming Nie. Quantum dot bioconjugates for ultrasensitive nonisotopic detection. *Science*, 281(5385):2016–2018, 1998.
- [137] Marcel Bruchez, Mario Moronne, Peter Gin, Shimon Weiss, and A Paul Alivisatos. Semiconductor nanocrystals as fluorescent biological labels. *science*, 281(5385):2013–2016, 1998.
- [138] W Russ Algar, Kimihiro Susumu, James B Delehanty, and Igor L Medintz. Semiconductor quantum dots in bioanalysis: crossing the valley of death, 2011.
- [139] 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.
- [140] 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.
- [141] 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.
- [142] 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.
- [143] 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.
- [144] 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.
- [145] bitcoinwiki. How bitcoin works.
- [146] Julio López and Ricardo Dahab. An overview of elliptic curve cryptography. Technical report, 2000.
- [147] wikipedia. Elliptic curve digital signature algorithm.
- [148] Adam Back. Hashcash - a denial of service counter-measure. Technical report, 2002.
- [149] B. Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. Wiley-India, 2007.
- [150] wikipedia. Sha-2.
- [151] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.
- [152] Pawan Sinha. Recognizing complex patterns. *nature neuroscience*, 5(11s):1093, 2002.

- [153] Bruce MacLennan. *Gabor representations of spatiotemporal visual images*. University of Tennessee. Computer Science Department, 1991.
- [154] Vernon B Mountcastle. The columnar organization of the neocortex. *Brain: a journal of neurology*, 120(4):701–722, 1997.
- [155] 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.
- [156] 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.
- [157] 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.
- [158] Teuvo Kohonen. Learning vector quantization. In *Self-Organizing Maps*, pages 175–189. Springer, 1995.
- [159] Daniel D Lee and H Sebastian Seung. Learning the parts of objects by non-negative matrix factorization. *Nature*, 401(6755):788, 1999.
- [160] Daniel D Lee and H Sebastian Seung. Algorithms for non-negative matrix factorization. In *Advances in neural information processing systems*, pages 556–562, 2001.
- [161] David Guillamet and Jordi Vitria. Non-negative matrix factorization for face recognition. *CCIA*, 2:336–344, 2002.
- [162] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum algorithms for supervised and unsupervised machine learning. *arXiv preprint arXiv:1307.0411*, 2013.
- [163] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *arXiv preprint arXiv:1611.09347*, 2016.
- [164] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. *arXiv preprint arXiv:1307.0401*, 2013.
- [165] 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.
- [166] Alexy Bhowmick and Shyamanta M Hazarika. Machine learning for e-mail spam filtering: Review, techniques and trends. *arXiv preprint arXiv:1606.01042*, 2016.
- [167] EMVCo. Emv specifications.
- [168] 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.
- [169] 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.

- [170] Jon Erickson. *Hacking: the art of exploitation*. No Starch Press, 2008.
- [171] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017.
- [172] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Cryptanalytic attacks on pseudorandom number generators. In *Fast Software Encryption*, pages 168–188. Springer, 1998.
- [173] 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.
- [174] 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.
- [175] 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.
- [176] 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.
- [177] 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.
- [178] 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.
- [179] IEEE. IEEE 802 Specifications.
- [180] 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.
- [181] Ivan B Djordjevic and Bane Vasic. Orthogonal frequency division multiplexing for high-speed optical transmission. *Optics Express*, 14(9):3767–3775, 2006.
- [182] Ye Geoffrey Li and Gordon L Stuber. *Orthogonal frequency division multiplexing for wireless communications*. Springer Science & Business Media, 2006.
- [183] ISO. ISO/IEC FDIS 11801.
- [184] 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.
- [185] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.
- [186] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*, 2002.

- [187] 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.
- [188] 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.
- [189] 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.
- [190] 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.
- [191] Mehdi Namazi, Giuseppe Vallone, Bertus Jordaan, Connor Goham, Reihaneh Shahrokhsahi, Paolo Villoresi, and Eden Figueroa. Free space quantum communication with quantum memory. In *Frontiers in Optics*, pages FF2C–3. Optical Society of America, 2016.
- [192] 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.
- [193] Josephine Dias and Timothy C Ralph. Quantum repeaters using continuous-variable teleportation. *Physical Review A*, 95(2):022312, 2017.
- [194] IDQuantique. *Clavis 2 Datasheet*.
- [195] IDQuantique. *Clavis 3 Datasheet*.
- [196] 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.
- [197] 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.
- [198] Sima Bahrani, Mohsen Razavi, and Jawad A Salehi. Orthogonal frequency-division multiplexed quantum key distribution. *Journal of Lightwave Technology*, 33(23):4687–4698, 2015.
- [199] Trabesinger. Quantum simulation. *Nature Phys*, 8:263–280, 2012.
- [200] Masuo Suzuki. *Quantum Monte Carlo methods in condensed matter physics*. World scientific, 1993.
- [201] Matthias Troyer and Uwe-Jens Wiese. Computational complexity and fundamental limitations to fermionic quantum monte carlo simulations. *Physical review letters*, 94(17):170201, 2005.

- [202] Alexander L Fetter and John Dirk Walecka. *Quantum theory of many-particle systems*. Courier Corporation, 2012.
- [203] Iulia Buluta and Franco Nori. Quantum simulators. *Science*, 326(5949):108–111, 2009.
- [204] 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.
- [205] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.
- [206] Seth Lloyd et al. Universal quantum simulators. *SCIENCE-NEW YORK THEN WASHINGTON-*, pages 1073–1077, 1996.
- [207] Fumiko Yamaguchi and Yoshihisa Yamamoto. Quantum simulation of the t–j model. *Superlattices and microstructures*, 32(4):343–345, 2002.
- [208] 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.
- [209] 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.
- [210] 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.