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

List of Tables

List of Figures

1 Introduction

2 Health

3 Security

4 Environment

5 Entertainment

6 Productivity

7 Conclusion

A Quantum Netflix

B Quantum Random Number Generator

C Quantum Processor

D Quantum Video Games

D.1 Introduction

Video games are one of the main sources of entertainment nowadays. From the 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 nowdays 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.

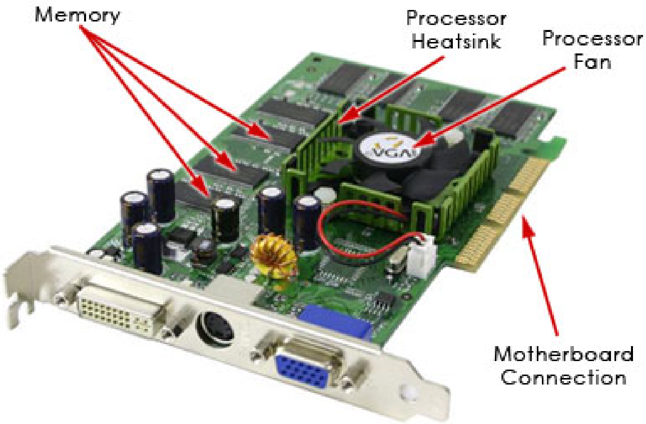


Figure D.1: A sketch of a GPU with some of its components.

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 [2], 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.2)). The unimprovable part of the game will greatly limit the quantum speedup.

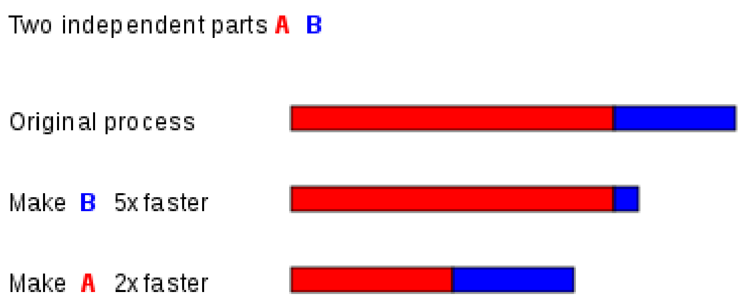


Figure D.2: Assume that a task has two independent parts, A and B. Part B takes roughly 25% of the time of the whole computation. By working very hard, one may be able to make this part 5 times faster, but this reduces the time of the whole computation only slightly. In contrast, one may need to perform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

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 [3, 4], Real Ket [5] and Flexible Representation of Quantum Images (FRQI) [6]. 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 [4, 6]:

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

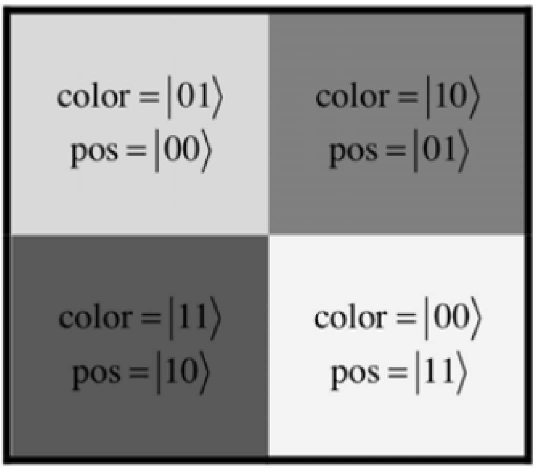
The real parameter encodes the frequency of the electromagnetic wave while is left uninitialized. Therefore our total state is

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

Coefficients α_{ij}, with $\sum_{j=0}^{2^m-1}|\alpha_{ij}|^2 = 1$ for all i with $0 \leq i \leq 2^{2n}$, are used to express the color of a pixel with position i by means of a superposition of all possible colors. For a given pixel i, coefficients α_{ij} take value 1 if the color of the pixel is j , and 0 otherwise. This is illustrated in Fig. (D.3) with a simple example of a 2×2 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 [7, 8] and computational geometry [9]. Even the important task of image segmentation found an quantum analogue based on quantum circuit schemes [10], 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 [11]. This translation was done by identify the RANSAC algorithm as a search algorithm, which



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

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

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

Figure D.3: Example of a simple 2×2 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 be possible, though, that a quantum system focused solely on graphics issues might be required, therefore it can possible to have quantum technologies impacting the video games industry before the advent of full quantum computer. One 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

Title: Quantum Enhanced Camera for Entertainment

Keyword tags: spatial resolution enhancement, quantum camera, photon entanglement

The idea of developing better and better cameras isn't new. Every year companies deliver professional cameras and cellphones with better resolution and characteristics, e.g. anti-blur modes, various focal planes, FOV. With an increasing number of amateur photographers, the camera and cellphones market will be pushed to deliver increasingly perfected technologies. The quantum technologies of the future can definitely improve the current limitations imposed by classical physics and produce better results. One characteristic that quantum technologies can improve when comes to cameras is their resolution. It has been shown that entangled photons can enhance the spatial resolution of imaging beyond the classical diffraction limit [1, 2]. By mapping the environment light into entangled photons and detecting them, all inside our cameras, which will require specialised detectors (single photon detectors), it can be possible to enhance the photo spatial resolution and improving its quality. Theoretically, it has been shown that N+1-photon entanglement improves the classical diffraction limit roughly by a factor of N (but it decreases the visibility by N) [2]. More specifically, considering the Airy disk, which is a description of the best focused spot of light that a perfect lens with a circular aperture can make, its classical radius is given by

$$\xi_{classical} = 0.61L/R,$$

where is light wavelength, Lis the distance between the object and the detector (or screen) and Ris the lens radius. For the quantum case, using N+1 entangled photons, the Airy disk radius is

$$\xi_{quantum} = 0.61L/RN,$$

which is N times smaller than the classical case and, hence, presents a sub-Rayleigh resolution. The straightforward advantage is a much better image quality compared to classical cameras. 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 q and p called quadratures. These quadratures have associated uncertainties given by the light state, which must obey an uncertainty principle like

$$\Delta q \Delta p \geq 1/4.$$

We say the light is squeezed along a given quadrature when the uncertainty of this quadrature is less than . This means that measurements using this quadrature will have a better sensitivity, and thus can image small objects more precisely than a classical source of light. This technique was used to image a living cell [5]. 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 [7]. 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 in information from the environment, it may mean entangling thermal light, but there has been some improvement in this direction over the past few years [3, 4]. 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 [8, 9], 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 avoid if one use 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 [10]. However being easier, it does not present the same improvement over sensitivity than the use of entangled photons does.

REFERENCES:

[1]: https://arxiv.org/pdf/0707.0268.pdf

[2]: https://arxiv.org/pdf/0812.2032.pdf

[3]: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1548851

[4]: https://journals.aps.org/pra/pdf/10.1103/PhysRevA.72.043805

[5]: https://journals.aps.org/prx/pdf/10.1103/PhysRevX.4.011017

[6]: https://www.nature.com/nphys/journal/v6/n6/pdf/nphys1652.pdf

[7]: https://arxiv.org/pdf/1605.08547.pdf

[8]: https://www.nature.com/nphoton/journal/v7/n12/pdf/nphoton.2013.287.pdf

[9]: https://arxiv.org/pdf/1606.06688.pdf

[10]: http://iopscience.iop.org/article/10.1088/0031-8949/91/5/053001/pdf

Title: Quantum Enhanced Camera for Health

Keyword tags: spatial resolution enhancement, quantum camera, photon entanglement

The advent of coherent light sources, e.g. lasers, and of better light detectors had a huge impact on medical areas. From cancer diagnosis [1], cancer treatment [2], melanoma treatment to scar revision, skin resurfacing, laser hair removal, tattoo removal [3], quantum technologies substantially improved health areas. The quantum technologies of the future can definitely improve the current limitations imposed by classical physics and produce better results. One characteristic that quantum technologies can improve when comes to cameras is their resolution. It has been shown that entangled photons can enhance the spatial resolution of imaging beyond the classical diffraction limit [4, 5]. By mapping the environment light into entangled photons and detecting them, all inside our cameras, which will require specialised detectors (single photon detectors), it can be possible to enhance the photo spatial resolution and improving its quality. A direct application would be in biological areas. This spatial resolution enhancement can be useful in blood tests [8, 9]. Theoretically, it has been shown that N+1-photon entanglement improves the classical diffraction limit roughly by a factor of N (but it decreases the visibility by N) [5]. More specifically, considering the Airy disk, which is a description of the best focused spot of light that a perfect lens with a circular aperture can make, its classical radius is given by

$$\xi_{classical} = 0.61L/R,$$

where is light wavelength, Lis the distance between the object and the detector (or screen) and Ris the lens radius. For the quantum case, using N+1 entangled photons, the Airy disk radius is

$$\xi_{quantum} = 0.61L/RN,$$

which is N times smaller than the classical case and, hence, presents a sub-Rayleigh resolution. The straightforward advantage is a much better image quality compared to classical cameras. 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 q and p called quadratures. These quadratures have associated uncertainties given by the light state, which must obey an uncertainty principle like

$$\Delta q \Delta p \geq 1/4.$$

We say the light is squeezed along a given quadrature when the uncertainty of this quadrature is less than . This means that measurements using this quadrature will have a better sensitivity, and thus can image small objects more precisely than a classical source of light. This technique was used to image a living cell [8]. 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 [10]. 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 in information from the environment, it may mean entangling thermal light, but there has been some improvement in this direction over the past few years [6, 7]. 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 [11, 12], 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 avoid if one use 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 [13]. However being easier, it does not present the same improvement over sensitivity than the use of entangled photons does.

REFERENCES:

[1]: https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/615aebb9234e4a3404

[2]: Goldman L (1990). "Dye Lasers in Medicine". In Duarte FJ; Hillman LM. Dye Laser Principles. Boston: Academic Press. pp. 419–32. ISBN 0-12-222700-X.

[3]: Costela A, Garcia-Moreno I, Gomez C (2016). "Medical Applications of Organic Dye Lasers". In Duarte FJ. Tunable Laser Applications (3rd ed.). Boca Raton: CRC Press. pp. 293–313. ISBN 9781482261066.

[4]: https://arxiv.org/pdf/0707.0268.pdf

[5]: https://arxiv.org/pdf/0812.2032.pdf

[6]: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1548851

[7]: https://journals.aps.org/pra/pdf/10.1103/PhysRevA.72.043805
[8]: https://journals.aps.org/prx/pdf/10.1103/PhysRevX.4.011017
[9]: https://www.nature.com/nphys/journal/v6/n6/pdf/nphys1652.pdf
[10]: https://arxiv.org/pdf/1605.08547.pdf
[11]: https://www.nature.com/nphoton/journal/v7/n12/pdf/nphoton.2013.287.pdf
[12]: https://arxiv.org/pdf/1606.06688.pdf
[13]: http://iopscience.iop.org/article/10.1088/0031-8949/91/5/053001/pdf

F Television

G Solar Cells

Inefficiencies in the energy storage of current solar cell technology are primarily a result of fluctuations in the light received by the photocell. Quantum heat engine (QHE) photocells that consist of two photon absorbing channels have theoretically been shown to supress these fluctuations, and this energy regulation increases the efficiency of energy conversion from solar energy incident on the photocell to electronic energy produced [12]. Moreover, green light has shown no regulatory benefit in this scheme, and therefore should not be absorbed by the photocell in the optimal case. Given that energy fluctuations can lead to similar inefficiencies in photosynthesis due to oxidative damage, it is possible that a similar quantum thermodynamic mechanism to the quantum photocell occurs in photosynthesis, resulting in the low absorption of green light in plants.

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. 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. Classical solar technology also utilises semiconductor material linked by a bandgap such that individual photons are absorbed, producing photoelectrons. 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. 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. 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.

In order to describe the power transfer and fluctuations of such a two channel photocell, we can consider that the two input channels a and b which absorb photons with energies E_a and E_b also absorb two different powers $u_a < u_b$. These channels are coupled by the transfer of electrons to the same output state with a lower energy, such that the energy difference in the 'machine' E_M is used to generate electronic power. Therefore, electrons excited by photons from the ground state $|g\rangle$ to an excited state $|a\rangle$ or $|b\rangle$ are transferred to the state $|x\rangle$, losing energy to phonons. This decay to state $|x\rangle$ is possible because fast charge transfer to the machine, governed by rates γ_a and γ_a, dominates over radiative recombination. From state $|x\rangle$ the energetic electrons in the machine can be used to generate electronic power $u_M = E_M\Gamma$ at a rate Γ causing them to decay to a low energy state $|y\rangle$ and eventually the ground state $|g\rangle$ at a rate γ_g. The ratio E_i/E_M is similar for $i = a, b$ which means that neither channel is energetically favoured. In terms of the number of photons absorbed in each channel per unit time, N_a and N_b, the input power from each channel is defined as $u_i = N_i E_i$ for $i = a, b$, and the output power from the machine is $u_M = N_M E_M$, where N_M is the rate of photons extracted from the machine. The photocell can be modelled by discretising time and considering the energy at a time step n to be given by the sum $\sum_{m<n} u_M$, and the mean and variance of this value can be given by the Central Limit Theorem. The variance can also be derived analytically by assuming that the average power output is given by the machine power $u_M = p_a u_a + p_b u_b$, where p_a and p_b are the respective probabilities of each channel in the photocell absorbing a photon. The variance is then given by $\sigma = p_a(u_a - u_a)^2 + p_b(u_b - u_M)^2 + (1 - p_a - p_b)u_M^2$ from the definition $Var(x) = \sum_i [p_i(x_i - \mu)^2]$. 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 λ and temperature T to be described by an irradiance spectrum $I(\lambda, T)$, the average input energy flux can be written as $u_i = \int A_i(\lambda)I(\lambda, T)d\lambda$, 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. It is possible to engineer semiconductor nanostructures with these properties, and therefore these structures could be promising candidates for light harvesting. 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. By electronic coupling of quantum dots, and by integrating these quantum dots into advanced heterointerface devices or metal nanoparticles, the increased power conversion efficiency as a result of two-channel absorption could be directly observable.

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 [13]. 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.

H Quantum Enhanced Material Detection

I 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 [14]. Nowadays the battery market is based in alkaline, lead-acid, and Lithium-Ion batteries and rapidly changing into an exclusively rechargeable battery market.

The recent Lithium-Ion batteries....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. Tesla now claims that a Tesla Model S battery cost is $240 per kWh and that the expected cost for a Model 3 is $190 per kWh. Soon battery packs will cost closer to $100 per kWh, which will make them essentially cheaper than all gas-powered vehicles.
[15]

However, despite the battery industry has been changing their technologies along time, they all share the same fundamental principle: Batteries convert chemical potential energy directly to electrical energy that we use to do some work. .[On the Carnot limit and 2nd law]...How can our understanding and control of quantum systems help us to improve batteries?

I.1 Information is the key

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 [16]) which allows extraction of work from one thermal bath. If one has a d-level system in a pure state ψ one can draw $kTln(d)$ work out of heat bath of temperature T. If a state of the system is a mixed state ρ, then the amount of work would correspond to

$$W = kTln(d) - TS(\rho) \tag{1}$$

where $S(\rho) = ks(\rho)$; $s(\rho)$ is von Neumann entropy and k is the Boltzmann constant [17]. The equivalence between work and information opens a new way of thinking about the thermodynamics of quantum systems.

A quantum battery could be seen as a small quantum mechanical system that is used to temporarily store energy to transfer is 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. A battery is a physical system that stores energy. The internal energy of a quantum system is given by $tr[\hat{\rho}\hat{H}_0]$, where $\hat{\rho}$ is the state of the battery and $\hat{H}_0$ is its internal Hamiltonian. The idealized process of reversible energy extraction is then governed by the system dynamics plus some fields that are only turned on during a certain interval of time.

Furthermore, it is possible to study quantum properties of compound systems. The work deficit.a new paradigm of investigation of correlations of quantum compound system was obtained...

J Gravity Sensors

K Quantum Magnetic Sensors

L Quantum Enhanced Chemical Sensors

M Quantum Pattern Matching

N 3D Data Optical Storage

O Quantum Teleportation

P Quantum Key Distribution

P.1 Introduction

With the advent of credit and debit cards, cash transactions are less and less frequent than they once were, with most cash being withdrawn from ATMs. 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.2 Classical Systems

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 [18]). Using a 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 indexed Transaction Authentication Numbers (iTANs), 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, CAPs/DPA and one-time passwords/iTANs, many of which involve either tampering with the device or a man in the middle attack [19, 20]. 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 is turn can just cause more complex attacks [21], with the potential to cause a continual battle between fraud and banks.

One way to help improve security would be to use a Quantum Random Number Generator (QRNG) [22] 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 [23] and so, may be broken in the future.

see ap- pendi QRN

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 [24] 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.3 The Quantum Solution

To get around this potential flaw, the ideas of Quantum Key Distribution (QKD) are used: instead of transmitting a series of bits, 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 sender and receiver and receiving a percentage of incorrect polarisations above a threshold value

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

Figure P.4: 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 [25]

after the protocol indicates an eavesdropper as shown in figure P.4 [25]. 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 [26, 27].

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.5, then into a receiver and measured [1] as shown in figure P.6. This technology already exists and is shown in figure P.7 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 could potentially be used to send the single photons through a fibre through a network to the bank.

refere quan-tum port ap-pendi

P.3.2 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

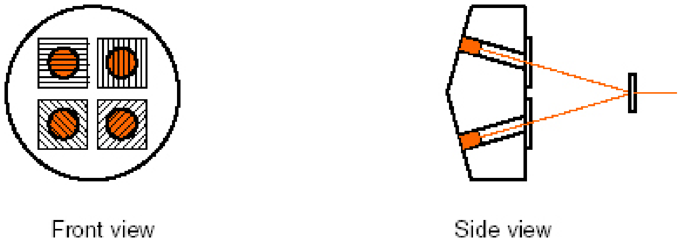


Figure P.5: 4 LEDs, attenuated to the single photon level, are placed behind polarisation gratings and angled to enter a diffraction grating at the same point, with the diffraction grating used to align the LED signals. Image taken from [1]

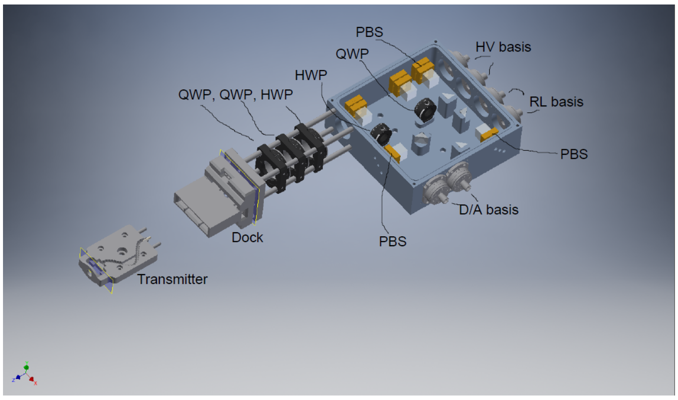


Figure P.6: Schematic of the receiving device used to perform handheld QKD. Image provided by David Lowndes

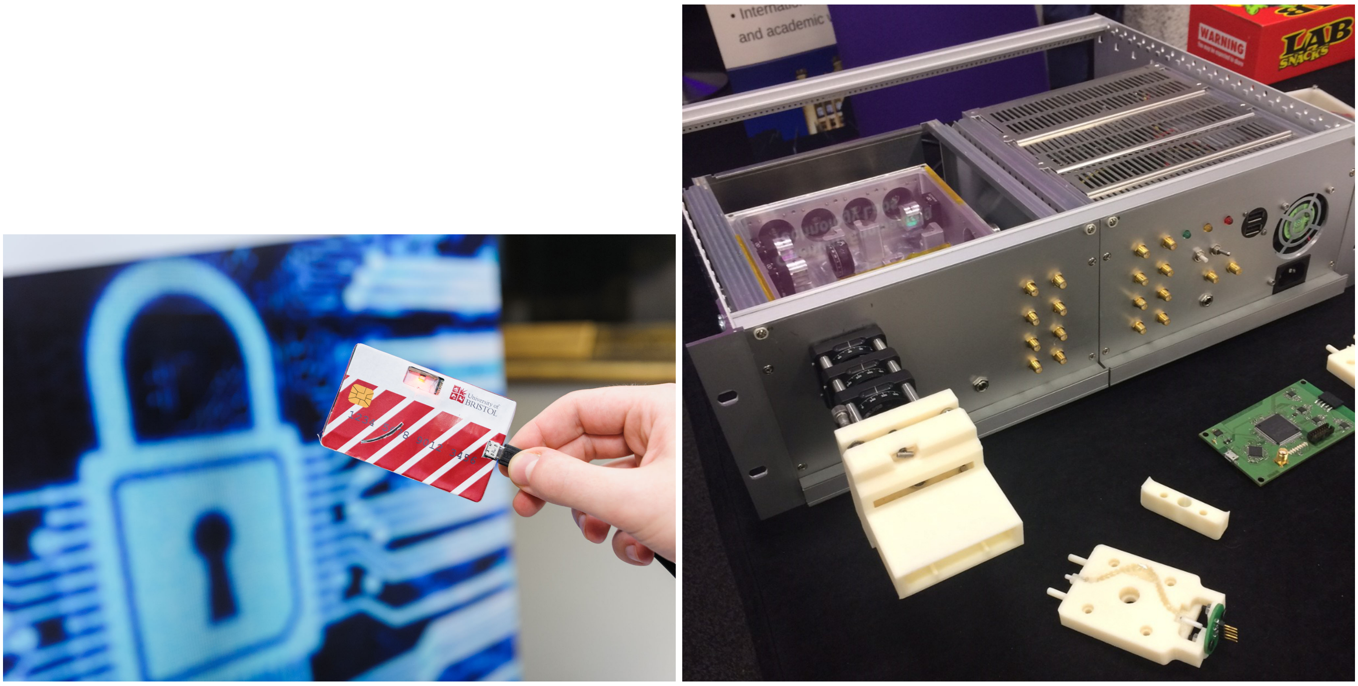


Figure P.7: Photos of the transmitting (left) and receiving (right) devices used to perform handheld QKD. Image provided by David Lowndes extra security due to the ‘key’ or only able to be copied by the receiver that knows the bases of the measurement (which can be decided by another random number).

Q Physically Unclonable Function

R Quantum Port Router

S Quantum Money

T Quantum Simulation

U Bacteria detection in the fridge

References

[1] 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.

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

[3] S. E. Venegas-Andraca and J. L. Ball. Processing images in entangled quantum systems. *Quantum Information Processing*, 9(1):1–11, Feb 2010.

[4] Salvador Venegas-Andraca and Sougato Bose. Storing, processing and retrieving an image using quantum mechanics. 5105, 08 2003.

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

[6] 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.

[7] 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.

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

[9] Marco Lanzagorta and Jeffrey K. Uhlmann. Quantum computational geometry, 2004.

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

[11] 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.

[12] 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.

[13] 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.

[14] Smithsonian Institution. Origin of Electrical Power. http://americanhistory.si.edu/powering/past/prehis 2002.

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

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

[17] 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.

[18] EMVCo. Emv specifications.

[19] 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.

[20] 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.

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

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

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

[24] 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.

[25] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and con tos5. 1984.

[26] 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.

[27] 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.