UNIVERSITY OF
BIRMINGHAM

Will The Qubit Become an Important Tool?

School of Physics and Astronomy
University of Birmingham

Josh Wainwright
UID:1079596

Project Supervisor: Dr. MJ Church
Date: November 2012

Word count: 5198 excluding latex commands.

Abstract

Some say that the qubit has the potential to revolutionise computing, allowing computing power to increase enormously. Others argue that the infrastructure we have built, and the familiarity with which we can relate to it, means that the classical bit is not going to be replaced.

In this essay, I will explore the potential of the qubit to become a useful tool, the challenges that are met in using it efficiently and some of the current and potential applications where they could make a significant impact. This area of computer science is extremely young and so predicting the direction it will take is impossible. However, the recent advances are proving that with time there is definite potential for this strange world to become everyday.

Contents

1 Introduction - What is a Qubit?

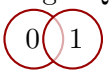
A qubit is the name given to the quantum mechanical unit of information, analogous to the bit used in regular information technology [1].

The regular bit is simply the name given to the position of a logic gate, when used in the context of computing, and is represented in the computer as either a 0, the gate being "closed", or a 1, meaning the gate is "open". The name comes from a contraction of the words binary digit and so qubit is a *quantum binary digit*.

Referring to the bit as corresponding to the state of a logic gate comes from the earliest computers, before the advent of the transistor, when mechanical valves were used to perform computations. Though this analogy falls down with modern computers where there are many different two state systems, it is useful in understanding the key concept which underlies modern computing - that a bit has exactly two possible states that it can exist in. These states can be described by many examples, on/off, up/down, positive/negative, in/out, etc; but it is important to remember that it must be one or the other.

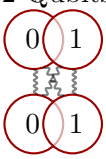
By contrast, the qubit, because of its quantum mechanical nature, has the two states described by the bit, but also has the possibility of existing in a superposition of these states. This superposition of the two classical states can be to any degree, meaning that there are effectively an unlimited number of states available ranging from completely 0 to completely 1 with every combination of them in between.

Single Qubit



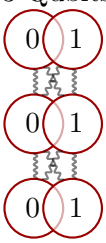
A single qubit can be in a superposition of two states. Compared to a classical bit, this is twice the amount of information.

2 Qubits



When two qubits are entangled, there is a possibility of 4 different states:
00, 01, 10, 11.

3 Qubits



When two qubits are entangled, there are 8 different states, so all the numbers from 0 to 7 can be encoded:

000,	100,
001,	101,
010,	110,
011,	111.

It would take a classical system 3 bits to encode just one of these numbers.

Figure 1: *Even with just three qubits, the encoding power is much higher. The cumulative effect of increasing the number of qubits is huge.*

2 Qubits - A History

Theoretical physicist Max Planck started the first work on quantum mechanics in the early 1900's when he described the quantum nature of radiation and then Erwin Schrödinger moved this work into a mathematical basis with his formulation of his famous, posthumously named, Schrödinger equation. The work of Alan Turing in 1946 [2] led to the development of potential computational systems though it was not until the late 1950's that anything resembling the structure of today's computers was designed. From this point to now however, though the speeds and memory models have moved on, there is little difference in the way that classical computers operate.

The basic units inside a computer are the semiconductors and, as these continue to shrink in size, the laws that are used to describe them and predict their behaviour will have to change. Whereas classical laws are sufficient to describe the electronic properties when the components are macroscopic in size, as the size decreases, quantum effects become more and more important and so the system must be treated as quantum not classical.

A major breakthrough in quantum computing came in the early 1970's when it was shown that a reversible Turing machine was theoretically possible [3] and then, in the early 80's, formulatable using quantum mechanics [4].

The first work into how the equivalent quantum mechanical gates might be created was carried out in the 1990's when the problems of de-coherence was also first met experimentally. When possible methods to overcome the limitations through error correction techniques were explored [5], the actual computer based on quantum effects was realised.

Much of the current work in this area is concerned with the development of algorithms that would take advantage of the possibilities governed by quantum mechanics. The easiest method, and the only available method in classical computing, is to encode a single bit into each qubit used. But the qubit offers the possibility to use entanglement so that neither qubit carries a well defined amount of information but instead the information is contained in the qubit's dual state.

This method of data transfer/storage means that other possible effects can be taken advantage of, including quantum teleportation and quantum error correction. These effects mean that the benefits of quantum computing are far greater than just increasing the density of gates on a chip or increasing the speed of calculations, but being able to perform calculations that would simply not be possible to program into a classical computer.

3 Qubits - A Basic Understanding

3.1 Mathematical Representation

The standard representation used in quantum information is using Dirac Braket notation and so we shall use this notation too. Using this notation, the superposition of a qubit in an arbitrary state is given by

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where the coefficients α and β are the amplitudes of the qubit in the 0 and 1 "directions" and Ψ is the resulting state.

As in all of quantum mechanics, this final state represents the full range of possible states, but gives no information as to what state the object would be in if it were measured, it provides only probabilities. The probability of any one state is given by the absolute amplitude of the coefficient for that state, so that from equation 1, the probability of measuring the qubit in the 0 state is $|\alpha|^2$ and the corresponding probability of it being in the 1 state is $|\beta|^2$. Since there are only two absolute states that exist and can be measured, there are constraints on the values that these coefficients can take. It follows that

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

simply because there must be a definite chance of measuring one or the other.

In order to represent the different states of the qubit, a Bloch Sphere is used, where the possible states are represented in 3-dimensional space on a unit sphere [1], figure 2. A qubit can be in a superposition such that it can exit at any point on the surface of the sphere.

The possibilities for the location of a state of a qubit is limited to two degrees of freedom, located to the surface of the sphere. The freedom comes from the complex nature of the coefficients α and β and is limited down from the expected four by the constraint in equation 2 and the fact that one of the coefficients can arbitrarily be set to be real since the overall state has no physical observable.

3.2 Physical Representation

The concepts that exist around the qubit work well to describe the idealised implementation, but actually devising a way to manufacture a physical qubit is very difficult. Several methods, which produce the desired effects, have been used. A few of these are summarized below, though many others have been reported.

Theoretically, any system that exhibits the binary states mentioned above and that is governed by quantum mechanics can be used to form a qubit, but it is the stability of those systems that will differentiate it from the others.

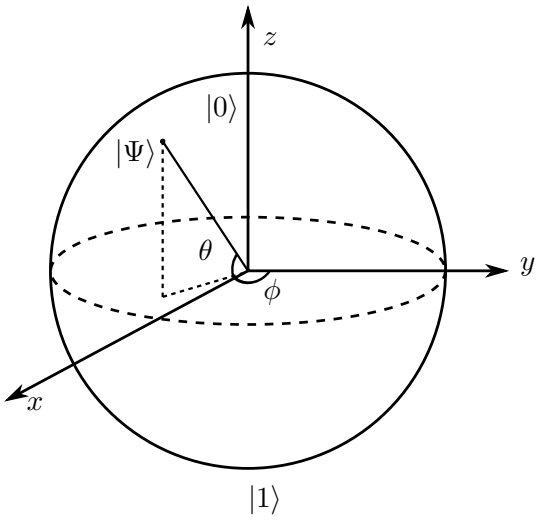


Figure 2: *The Bloch Sphere is used to represent super-positioned states of a qubit. In this example, the probability amplitudes are given by* $\alpha = \cos\left(\frac{\theta}{2}\right)$ *and* $\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$ *[6]*

Name	Method	$\|0\rangle$	$\|1\rangle$
Photon [7]	Polarization	Vertical	Horizontal
Josephson Junction [8]	Super conducting charge qubit	Clockwise current	Anti-clockwise current
Electron [9]	Electron Spin	Up	Down
Quantum Dot [10]	Dot Spin	Down	Up

3.3 Quantum Bit Example

We can demonstrate some of the strange qualities of the qubit easily using the mathematical representation introduced above. We shall consider a trine. This is simply the name given to a qubit that can be in one of the three states listed below and can be thought of as an extension of the classical bit, but with limitations on the qubit.

$$|\Psi\rangle = |0\rangle$$
$$|\Psi\rangle = \tfrac{1}{2}|0\rangle + \tfrac{\sqrt{3}}{2}|1\rangle$$
$$|\Psi\rangle = \tfrac{1}{2}|0\rangle - \tfrac{\sqrt{3}}{2}|1\rangle$$

If this were to be implemented using, for example, the photonic qubit, these three states could be thought of as polarisation of the qubit in the vertical direction, $30°$, or $-30°$. Each of these states is equally likely.

Since there are three possible states, in classical theory, a trine encodes

$$\log_2 3 \approx 1.585$$

bits worth of information. This is an improvement on a classical bit since this 1 qubit can hold more than 1.5 bit, however, quantum mechanics rules out the measurement of the qubit precisely. This reduces the possibility of knowing the state to just two of the three options, leaving one bit of uncertainty. Thus we can read

$$(\log_2 3) - 1 \approx 0.585$$

of information. So this is in fact a reduction in the amount of available information. Suppose now, we have two identical trines. It has been shown that for this system, the available information increases to

$$\tfrac{\sqrt{2}}{3}\left(1 + \log_2(17 + 12\sqrt{2})\right) \approx 1.369$$

This is more than 2×0.585, the previous result for a single measurement. So we have a situation where it is possible to read more than twice as much information from two identical qubits than it is to read the information from either one alone. This is a phenomenon that has no counterpart in the classical world.

4 Qubits - Plausibility

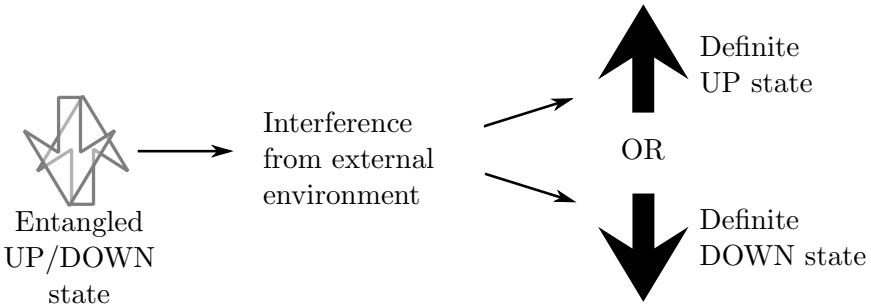
4.1 Disadvantages

Though it is proving to be one of the most successful theories of all time, in terms of experimental prediction and verification, quantum mechanics is also relatively young.

This is not a bad thing, since it has many more applications to be applied to and has the potential to continue reshaping the theories we have for the universe. But it does mean that, in the even younger field of quantum computing, there are several key issues that would hold the quantum computer back from becoming a widespread application of this powerful area of science.

4.1.1 De-coherence

One of the most important problems with quantum computing, and specifically with the manufacture and use of a physical qubit is the issue of de-coherence. This is the loss of the quantum properties that the quantum computer would rely on, so that the components of the qubit return back to a purely classical state. Or, in other words, a loss of information from the system into the surroundings. It occurs when two objects, photons, electrons, etc; that are entangled in a quantum system are disturbed and lose their entangled state. De-coherence is a major problem for the application of qubits to the quantum computer since the computer would have to rely on being able to store and then retrieve information in order to perform calculations and so would require the quantum system to remain coherent. The environment that surrounds the system is out of control and so any information that is passed there is lost.



The issue facing scientists is that it can be initialised by any smallest interaction with the surrounding environment or system. This means that, currently, the only way to avoid de-coherence is to try to keep the entire quantum system completely isolated. Because of the delicacy of the quantum state, the sort of interaction that can produce de-coherence is very small, such as slight temperature changes, or the collision of single atoms or molecules.

Generally a quantum state will remain coherent, and so useful for applications in quantum computing, for a tiny length of time. De-coherence was first discussed in 1991 [11], but still the best efforts have only extended the time before loss of information to 180 seconds [12]. Though this is a huge move forward from the milliseconds achievable only a few years ago, even this is quite an exaggeration since it relates to simply ensuring the qubit exhibits the necessary properties. As well as this, it also requires the system, and so equipment required, to operate at fantastically low temperatures with the

aim of removing as much as possible of the external interference. The current record for actually storing any information and retrieving it again from such a system at roughly room temperature is far shorter, of the order of 1 second [13].

One of the driving motivations for finding new ways of realising the qubit through different mechanisms is that the de-coherence times vary depending on the type of qubit used. For example, consider the photon qubit. This involves trapping an infra-red photon in an optical fibre. This has one of the shortest maximum coherence times, around 0.1 ms. This is due to the extreme requirements of the system in order to preserve the quantum state; the optical fibre must be of extremely high quality and the photon must have exactly the frequency for which the fibre is the most transparent. This adds up to a huge challenge to extend the lifetime of these qubits.

On the other hand, the nuclear spin of the small number of ^{29}Si atoms in ^{28}Si can have a much higher lifetime, at least 25 seconds. Again this is due to the way these qubits are structured, this time being much more resilient to external interference.

4.1.2 Error Correction

In the classical computer, there are errors introduced to the calculations simply by the flow of electrons through wires and the fact that components are not perfect meaning information can be distorted or lost as it passes through them. This can happen as the information about a piece of data is moved from one component to another, or within a single component. The data is transferred as single bits and so the change of a bit, from "1" to "0" or vise versa, is known as bit-flipping. The build up of these errors and successive bit-flips leads to noise that can distort an image or sound or cause a calculation to be incorrect. To counter this effect, which could be very serious if the computer is controlling important information or equipment, error correction is introduced.

The simplest type of classical error correction involves using the mathematical concept of redundancy. This involves increasing the number of times each bit is sent, so that, if one of those copies is damaged, there are still intact versions that can be relied on. Consider a piece of information being used inside a computer, for example the binary code,

001011101

If this information was sent again with redundancy, this might now look like,

000 000 111 000 111 111 111 000 111

Now, if the first packet of 3 bits, representing the single bit, '0', is changed en route, so that now it contains '010', the receiver can compare the three bits in the group and use the bit that represents the majority of the three. In other words, there are still two remaining '0' bits and only one distorted 1 bit, so the '0' will be used, overcoming the error in transmission.

This method is very effective for the classical example, but when applied to a quantum computer, is not transferable. One reason for this is that, in order to determine which was the correct unaltered state, each of the three qubits would have to be measured and then compared. But the quantum nature of the states would mean that the simple act of measuring would destroy their states and so not give an accurate representation. Secondly, the fact that the qubits can be in a superposition of different states means that there is a far greater, in fact infinite, number of different possible values that could be measured, and so a much greater scope for error. This would mean that a much higher number of qubits would have to be transferred in order to have enough states to compare with and know that the majority had not been subject to error.

4.2 Qubits - Advantages

We have discussed a few of the major disadvantages, though as time goes on, these are becoming fewer and fewer. As our understanding of the quantum behaviour of systems increases, so does our ability to manipulate it. Though most would agree that there is a long way to go, and that it is going to take some huge developments in technology and what it can provide to allow quantum computing to get to the point that classical computing has reached, there is potential.

4.2.1 Error Correction

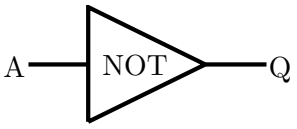
We saw previously how error correction can be easily implemented in a classical system using redundancy, but the quantum qubit means that this form of detection for the occurrence of errors is not possible. Despite this, there are still ways of overcoming the errors that are inevitably introduced to a system when it is exposed to the natural environment.

Before we can understand how error correction can be applied to the quantum bit, we first need to know how the quantum equivalent of some of the logic gates used in classical computing work. Logic gates are the neurons to the brain that is the computer's CPU. They are gates that sometimes allow information to pass through them in certain configurations, and in others change the information if it has the right characteristics. Two simple examples are the AND and the NOT gate. The AND gate receives two streams of data and does a simple binary addition, whereas the NOT takes a single input and inverts it so that the opposite is produced. The tables that describe these gates are shown below as they are the basis of the quantum computer as well as the classical.

Instead of these classical gates, a quantum computer uses variations that operate through different physical processes, but which provide the same results. However, the most useful logic gate for dealing with qubits turns out to be the CNOT gate. This is short for *controlled*-NOT gate as it takes a second input as a control bit. This means that if

Input		Output
A	B	Q = A AND B
0	0	0
0	1	0
1	0	0
1	1	1

Figure 3: *This is the truth table for the AND logic gate and the circuit symbol.*



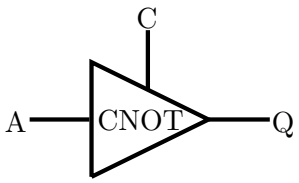
Input	Output
A	Q = NOT A
0	1
1	0

Figure 4: *This is the truth table for the NOT logic gate with the circuit symbol.*

the value of the control is "1", then the output is the reverse of the input. If the control is "0", then there is no change.

Input		Output
A	C	Q = CNOT A
0	0	0
0	1	1
1	0	1
1	1	0

Figure 5: *This is the truth table for the AND logic gate and the circuit symbol used.*



We shall consider a qubit that is in a superposition of states such that

$$|\Psi\rangle = \big(\alpha|0\rangle + \beta|1\rangle\big)|00\rangle. \tag{3}$$

This state represents a qubit that is in a superposition state with coefficient α in the 0 direction and β in the 1 direction along with two extra qubits that are in a definite state of $|0\rangle$. These last two qubits act as the extra comparison bit that were used in the classical example. We then pass this function through two CNOT gates, one after the other using one of the extra qubits for the control for the first and the other for the second gate. When this is performed, the resulting function is

$$|\Psi\rangle = \alpha|000\rangle + \beta|111\rangle \tag{4}$$

This is now a superposition of the three qubits. All three of the original qubits exist still, but are now locked together in a single state.

This is the intermediate state when the qubits would be checked for errors. To test this, let us imagine that one of the qubits underwent a bit-flip during transmission and now

we want to discover the original message. If we flip one of the bits in this state we might get

$$|\Psi\rangle = \alpha|0\underline{1}0\rangle + \beta|1\underline{0}1\rangle \tag{5}$$

The same elemental contribution in each direction will be affected and so only one has changed, the middle in this case. We will keep track of the errors with an underline. This state then is known to contain an error but it still also contains the extra qubits that were added for redundancy. To remove them, the state is passed once again through a pair of CNOT gates. For this case the result is

$$|\Psi\rangle = \alpha|010\rangle + \beta|1\underline{1}0\rangle \tag{6}$$

This time, only the β contribution was changed since the control bit was 0 and so allowed a change. The control bit for the α part was 1 so there was no change there. But now we have a situation where the entangled state can be decomposed. Both of the 0 and 1 directions have the same last 2 qubits. This means that they can be separated out leaving

$$|\Psi\rangle = \big(\alpha|0\rangle + \beta|1\rangle\big) \times |10\rangle \tag{7}$$

We can summarise this process as shown in figure 6. This diagram shows each step of the error detection and correction with each CNOT gate and the addition of a final gate called a Toffoli gate. This is used for more general error correction and has no effect on this case.

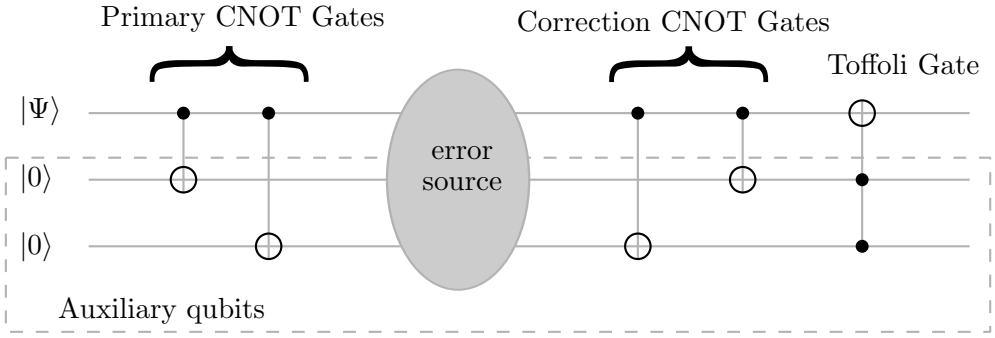


Figure 6: *Even with just three qubits, the encoding power is much higher. The cumulative effect of increasing the number of qubits is huge.*

4.2.2 Integer Factorisation

Another keenly investigated benefit of quantum computing would be the possibility for efficient, large digit, integer factorisation. Integer factorisation involves the splitting of numbers down into their prime factors. For example, figure 7 shows how the number 864 is factorised.

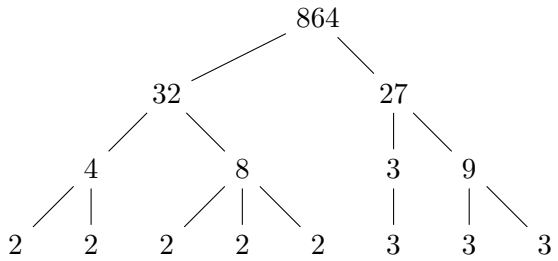


Figure 7: *The number 864 factorised by hand into component prime numbers which can be written in shorthand as $2^5 \times 3^3$. The application of this is used in encryption for situations like on-line banking, and for modelling large systems like weather systems.*

Though this is fairly trivial to perform by hand for small numbers, for large numbers, there exists no efficient algorithm that is able to split numbers in such a way. For example a 232 digit number was successfully factorised by a group of researchers in 2009, though this required the combined input of "many hundreds of machines" and took almost 2 years [14]. This factorisation was concerned with an RSA encryption key and demonstrates the security of the RSA encryption method - on a standard classical computer this would take of the order of 1500 years.

Though this slightly contrived example demonstrates the principle that large numbers are difficult to factorise, it also includes reference to one of the reasons that efficient factorisation methods are sought. Almost all modern encryption methods rely on the use of large numbers, that are very difficult to factorise, to lock the information they relate to. Using this method, a computer has to guess or calculate the prime numbers that make up the key in order to break the encryption, and as such is very difficult and time consuming to do.

The quantum computer however, would provide the necessary computational skill to be able to tackle this problem. As was discussed previously, it is not the increase in computing *power* that would make a quantum computer able to tackle problems, but instead, the superposition of multiple different states simultaneously that could allow these problems to be solved. There are already a number of different mathematical algorithms that have been written specifically to tackle the integer factorisation problem on a quantum computer.

One of the earliest of these is Shor's algorithm, named after its designer Peter Shor [15]. This algorithm sets out simply to solve the following problem,

Given an integer N, find its prime factors.

Utilising the possibilities of the quantum computer, Shor was able to demonstrate that his algorithm can factorise a given digit in polynomial time [15], i.e. the time that the algorithm takes to finish is polynomial in $\log(N)$, where N is the size of the input value. Compared to the fastest classical versions, this is exponentially quicker.

Shor's algorithm achieves this by utilising the fact that a quantum state can be in a number of states simultaneously. This means that the value of several calculations can be superposed and tested simultaneously. Though the no-cloning theorem, which prevents a quantum system from being identically reproduced [16], allows this technique to be performed exactly, an estimate using a Fourier transform of the original waveform is enough to allow the algorithm to find the factors much quicker than any classical technique.

4.3 Safe Transfer

We have seen some of the ways that the qubit can be used to perform applications that exploit the quantum nature of the qubit through the application of mathematics to manipulate them. But there are some fields of quantum computing that the qubit simply creates because it has properties that had never been considered before.

The major example of this, and a huge driving force behind much of the research into quantum computing, is the possibility of completely safe, 100% secure information transfer through quantum cryptography. This application uses qubits in the form of polarised photons, the polarisation of which controls the state that the qubit occupies.

Cryptography involves the transfer of information using a secret code that allows the sender to encode, and then the receiver to decode, a message or set of information. Currently, the most widely used and most secure method of cryptography is called asymmetric public key cryptography, figure 8. This involves a pair of keys that are used, one to lock and the other to unlock the information. The locking key is sent publicly since all it can do is encode the data. The unlocking key is kept secret by the receiver. This means that the key to unlock the information is never in the open.

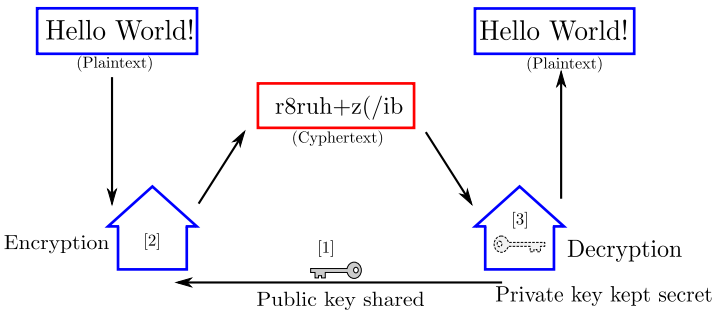


Figure 8: *In asymmetric key cryptography the plain-text is encoded,* [2]*, using the public key sent by the receiver,* [1]*, then sent as cypher-text to be decrypted with the private key which stays with the receiver at all times* [3].

This has proved to be an extremely secure method of sending data and is currently used by many banks and other industries to pass information and data with a minimum possibility of a breach of security. However, it is not impenetrable. Since the encryption

and decryption keys must match each other, it is theoretically possible to calculate what the decryption key must be if one has the encryption one. As well as this, there is always the brute force method, which simply involves trying every possible combination of arrangements of the code to unlock the data until the correct one is found by elimination. Though this was unthinkable a few years sago, because of the size of the keys used, modern computers and networks of computers working together are starting to have the capabilities to break into these locked safes of information.

This is where quantum cryptography is different. Instead of having a key with more and more digits, hoping that this will make the lock more and more difficult to guess the correct key, quantum cryptography employs the Heisenberg Uncertainty Principle. The uncertainty principle states, in one of its forms, that:

> It is impossible to measure simultaneously both the position and velocity (or momentum) of a microscopic particle with absolute accuracy or certainty.

This can be extended to the measurement when it takes place, observing the fact that the inaccuracies are introduced into the system, so that the principle can be stated as:

> It is not possible to measure or observe a particle system without disturbing that particle or system in some way.

Analysis of this principle shows that there is another important rule of quantum mechanics here, that an arbitrary quantum state can not be copied exactly since this would involve first knowing the exact state of the system that was to be copied. This is important since it means that any attempt to eavesdrop on any information transfer can be detected as soon as the data is received.

4.3.1 BB84

We will examine the most commonly investigated method of quantum cryptography called BB84, so called after its inventors, Charles Bennett and Giles Brassard and the year they developed it, 1984 [17].

The principle of sending quantum encoded information is fairly simple. The key that locks the information to be sent is encoded as qubits of light using the polarisation in the vertical and horizontal directions and the left and right diagonal directions to be either a “0” or “1”. These are called baseis, the first is the rectilinear basis, the second is the diagonal basis. A third possibility is the circular basis where the polarisation is either right- or left-handed.

The key is sent to the receiver using one of the two settings randomly. For each value of the qubit, a different direction is defined, for example the arrangement shown in table 1.

The sender creates a random bit and then selects one of the basis sets to encode it in. This is repeated for each bit in the set. For each qubit sent, the sender takes note of the

Basis	0	1
+	↑	→
×	↗	↘

Table 1: *One possible arrangement of the two baseis + and × and their corresponding qubit encoding.*

randomly selected basis.

The receiver then makes measurements randomly of the qubits that have been sent using two analysers that detect if the qubit is polarised in the vertical/horizontal direction, or the diagonal direction. The sender does not reveal which direction setting was used to encode the "0"s and "1"s, meaning that the receiver and so also any eavesdropper does not know either. When the receiver measures the information, quantum uncertainty means that half of the time the right answer is found. This is due to the baseis not being orthogonal to each other and so a quantum measurement cannot determine between them. After the measurement, the photon is left in the state that it was measured to be in so an eavesdropper would affect the data being sent.

The receiver does not know how the data was encoded so can at most only select at random which basis set to assign each qubit measured. After the information has been received, the sender releases the settings for the analyser so that the receiver knows which basis set was used for each individual qubit. The receiver can then correctly pick out the key from the results. On average, the correct value will have been found half of the time and the measurements where the correct answer is not found are discarded. The remaining bits constitute the shared key that the two parties can use, knowing that no-one else can have intercepted the transmission of the key.

Sender's random bit	1	0	1	0	0	1	1	1
Sender's random sending basis	+	+	×	×	+	+	×	+
Polarisation sent	→	↑	↘	↗	↑	→	↘	→
Receiver's random measuring basis	+	×	×	+	+	×	+	+
Polarisation receiver measures	→	↗	↘	→	↑	↗	→	→
The settings are shared by the sender								
Shared secret key	1		1		0			1

One of the first experimental demonstrations of quantum cryptography was carried out in 2000 by a group at the University of Vienna using pairs of entangled photons [19]. They transmitted the encoded qubits over a distance of 360 m via an optical fibre showing that the principle is definitely possible. However, the errors in transmission and measurement meant that they were unable to extend the distance the data was transferred. In 2004 though, another group from Toshiba Research at Cambridge managed to securely encode, transfer and decode a still image over a distance of 122 km via a standard Telecom cable [20]. Figure 10 shows the images that was transferred as well as the two keys that were generated and the decoded image. The small remaining errors in the image can

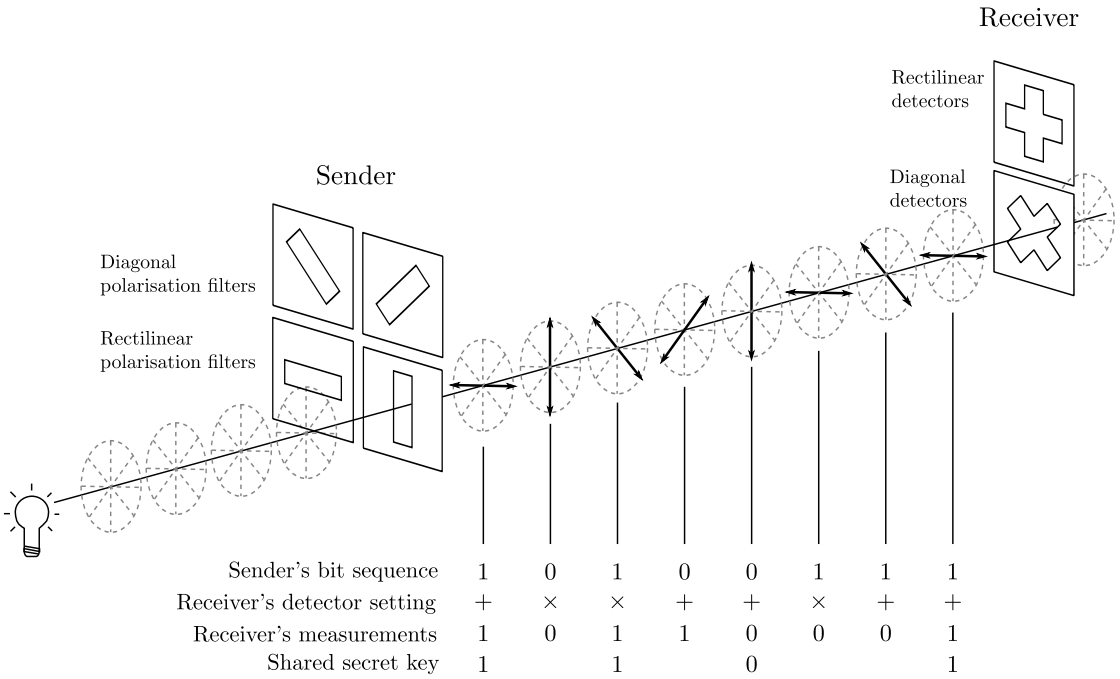


Figure 9: *Using two different polarisation baseis to send a set of qubits securely [18].*

be seen as defects to the colour, but overall, the image is very clearly the same as was transmitted.

5 Qubits - Conclusion

We have seen how the many advancements in quantum theory have changed the way that we think about the world on a small scale. This is being applied more and more to the macroscopic scale, allowing us to take advantage of some truly extraordinary discoveries. There are also some very serious hurdles that need to be tackled. We have discussed a few here, but there are many that prevent quantum computing being used widely. As each new advancement is made there are always a number of new challenges that require work to overcome.

But the advances are starting to find uses, and are being implemented into the real world for industrial and commercial applications. In 2010 the FIFA World Cup in South Africa used a version of the quantum cryptography discussed in section 4.3 to secure the transmission of videos, e-mails, and phone calls that were regularly relayed between the stadium and the nearby centres for police, fire-fighters, and military personnel. This demonstrated a trust in the very new technology that is needed for the expansion out of the research environment into general usage.

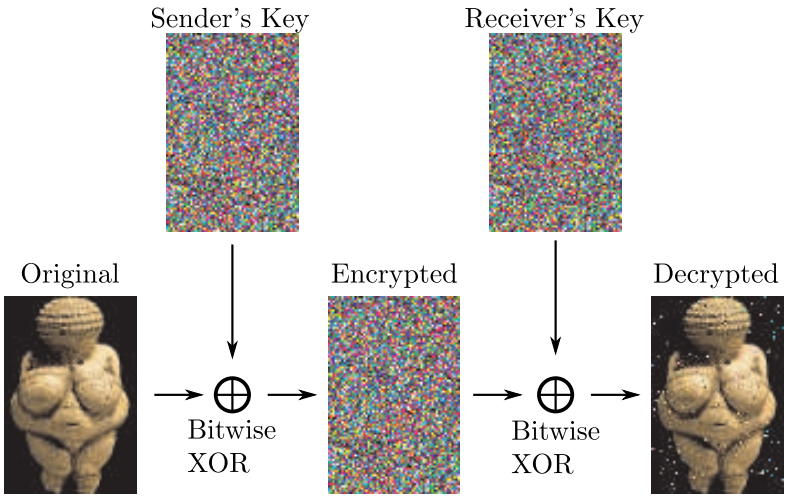


Figure 10: *An image of the "Venus von Willendorf" effigy was transferred via a standard Telecom cable using polarised photon qubits and quantum cryptographic encoding.*

Trust is an issue that several new areas of physics lack in the public eye, that prevents them, in many people's view, from becoming more mainstream. The reputation of nuclear power, for example, once it was properly understood what was going on, was seriously damaged by the disasters at Chernobyl and more recently Fukushima Daiichi. It is a reputation like this that would prevent quantum theory in the field of computing and telecommunications from becoming the industry standard.

It is to quantum theory's advantage, therefore, that the word "quantum" is quickly becoming a media 'buzz-word' because of the visually and theoretically impressive advancements that scientists are able to offer in this area. People are keen to show their interest in this field and companies are able to take advantage of this by directing money and effort into research programs to feed a desire for this new and exciting technology.

If quantum theory and it's associated sciences are able to keep up this interest and the level and significance of the funding and potential that it is currently showing, then the recent trends indicate that the quantum binary digit will play an even more significant role in daily life, perhaps, one day, surpassing the plain old classical bit.

References

[1] E. Rieffel and W. Polak. *Quantum Computing, A Gentle Introduction.* The MIT Press, Massachusetts, 2011.

[2] B. Jack Copeland. *Colossus: The secrets of Bletchley Park's code-breaking computers.* Oxford University Press, 2006.

[3] C.H. Bennett. Logical reversibility of computation. *IBM journal of Research and Development*, 17(6):525–532, 1973.

[4] P. A. Benioff. Quantum Mechanical Hamiltonian Models of Discrete Processes That Erase Their Own Histories: Application to Turing Machines. *International Journal of Theoretical Physics*, 21:177–201, April 1982.

[5] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[6] Smite-Meister, 2009.

[7] Zong-Quan Zhou, Wei-Bin Lin, Ming Yang, Chuan-Feng Li, and Guang-Can Guo. Realization of reliable solid-state quantum memory for photonic polarization qubit. *Phys. Rev. Lett.*, 108:190505, May 2012.

[8] A. Barone and G. Paterno. Physics and applications of the josephson effect. *JOHN WILEY & SONS INC., 605 THIRD AVE., NEW YORK, NY 10158, 1982, 592*, 1982.

[9] R. Hanson, L. P. Kouwenhoven, J. R. Petta, S. Tarucha, and L. M. K. Vandersypen. Spins in few-electron quantum dots. *Rev. Mod. Phys.*, 79:1217–1265, Oct 2007.

[10] Daniel Loss and David P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A*, 57:120–126, Jan 1998.

[11] Wojciech H. Zurek. Decoherence and the transition from quantum to classical. *Physics Today*, 44(10):36–44, 1991.

[12] M. Steger, K. Saeedi, M. L. W. Thewalt, J. J. L. Morton, H. Riemann, N. V. Abrosimov, P. Becker, and H.-J. Pohl. Quantum information storage for over 180 s using donor spins in a 28si "semiconductor vacuum". *Science*, 336(6086):1280–1283, 2012.

[13] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, D. J. Twitchen, J. I. Cirac, and M. D. Lukin. Room-temperature quantum bit memory exceeding one second. *Science*, 336(6086):1283–1286, 2012.

[14] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery,

Dag Arne Osvik, Herman Te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit rsa modulus. In *Proceedings of the 30th annual conference on Advances in cryptology*, CRYPTO'10, pages 333–350, Berlin, Heidelberg, 2010. Springer-Verlag.

[15] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE, 1994.

[16] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, October 1982.

[17] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John A. Smolin. Experimental quantum cryptography. *J. Cryptology*, 5(1):3–28, 1992.

[18] Simon Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Anchor, August 2000.

[19] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84:4729–4732, May 2000.

[20] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84(19):3762–3764, 2004.