Quantum networking, and its future applications in online gaming

Elliot Reece Walker[1][0000-0002-4683-0662]

[1] University of Brighton, Sussex, United Kingdom
E.walker5@uni.brighton.ac.uk

Abstract. This paper comprises of descriptive research conducted towards the current state of quantum computing methodologies in networking, accompanied by a proposal of how they may be applied to online games in the future to mitigate the effects of latency and cyber-attacks.

Keywords: Cyber-security · Gaming · Latency · Networks · Quantum

1 Introduction

1.1 Issues in modern online game networks

Multiplayer networks may possess $1\colon 1$, $1\colon n$, or $m\colon n$ client connectivity, usually facilitated with either UDP (User Datagram Protocol) or TCP (Transfer Control Protocol) over a Star topology. With this common architecture, common issues and inefficiencies arise:

1. **Network latency:** Commonly referred to as “lag”. It affects the time over which in-game events are processed between clients (players) due to their separation distance, the number of clients connected, the bandwidth each one possesses, the network topology facilitating their connection, and the quantity of data lost throughout its journey from origin to destination.

   Approaches to addressing latency involve applying connectionless protocols to sacrifice stability for speed, or by utilizing appropriate network topologies which have a direct impact on data efficiency (Omni.Sci, 2020). Network latency is particularly troublesome in competitive settings where a consistent flow of gameplay and reliable connectivity are desired.

2. **Cyber-attacks:** Whilst data shared between clients may be encrypted it is not impervious to being intercepted and decrypted by eavesdroppers. Online games seldom come without the ability for users to make in-game purchases or communicate directly with others: any exchanges made can be intercepted by malicious hackers who will accumulate and exploit their personal information, such as payment details or passwords.

1.2 Quantum computing

Quantum computing is a paradigm of computation first conceived in 1980 by Paul Benioff, where in a paper written for the Journal of Statistical Physics (Benioff, 1980, pp.563-591) he described the framework for a Turing Machine that incorporates aspects of quantum mechanics: a theory which enables statistical predictions to be made on the behaviour of microscopic particles (Scherer, 2019, pp.11). Akin to how classical computing at its most basic level can be summarised with binary logic, quantum computing can be summarised with a similar system.

The quantum of computational data in classical computing is the bit (binary digit), the equivalent in quantum computing is the qubit (quantum bit). A bit is facilitated by electricity, and a qubit is facilitated by a photon (a particle of electromagnetic radiation). Where a bit may possess a value of either 0 or 1 (low voltage, high voltage, etc.), a qubit may possess an infinite range of possible values due to its underlying quantum mechanics. Qubits exhibit a physical property known as **superposition**, which arises from the **Heisenberg Uncertainty Principal**: until a particle's quantum state is measured it may be considered as either value A or B. The superposition can be described mathematically as:

$$\boldsymbol{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$$

where $|0\rangle$ and $|1\rangle$ are the base quantum states $\begin{bmatrix}1\\0\end{bmatrix}$ (classical 0) and $\begin{bmatrix}0\\1\end{bmatrix}$ (classical 1) respectively, and α and β are their amplitudes, which are complex numbers associated with their quantum nature. The probability of measuring a particular quantum state can be calculated from the modulus of its amplitude squared: $P_\alpha = |\alpha|^2$, $P_\beta = |\beta|^2$. The probability of measuring a value is always 100% as per **Born's rule** and can be expressed as the sum of these probabilities: $P_\alpha + P_\beta = 1$. Born's rule dictates that the superposition of a system of n qubits is equal to the sum of the products of each state's amplitude a_i and its probable value $|i\rangle$, from $i \in \{0, 2^n - 1\}$, where 2^n represents the number of possible value combinations the system may possess for n qubits (Cacciapuoti, et al., 2020, pp.3811):

$$\boldsymbol{|\psi\rangle_{sys} = \sum_{i=0}^{2^n-1} a_i|i\rangle}, \qquad \boldsymbol{a_i \in \mathbb{C} : \sum_{i=0}^{2^n-1} |a_i|^2 = 1}$$

A two-qubit system consists of $2^2 = 4$ possible combinations (Hidary, 2019):

$$\boldsymbol{|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \qquad |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \qquad |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \qquad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}}$$

and adopt related but different forms when expressed as column matrixes.

Once a qubit's quantum state is measured classical binary data is produced as output. Quantum computing involves taking advantage of this probabilistic nature – it is possible to manipulate it (almost) deterministically: while which values are measured cannot be controlled, the probability of measuring a value can with **amplitude amplification**.

The superposition of a qubit consists of another component: the **relative phase** between the states, which arises from the way in which the superposition can be expressed as a point on the surface of a **Bloch Sphere**. Relative phase is defined as the angle about the imaginary axis of the Bloch Sphere. It can be altered independently from its amplitude, where the advantage of this is only observable is multiple qubit systems: by altering a qubit's relative phase its probability of being measured as either 0 or 1 can be indirectly affected. Alterations to relative phase are achieved through the application of **quantum gates**, which may be applied, mathematically, via matrix multiplication, and unlike their classical counterparts are entirely reversible. The following gates are considered the most fundamental:

- **NOT Gate:** The **NOT** gate is unary and flips the value of a qubit's superposition, such that the probability of measuring value A is replaced with that of measuring value B, and vice versa.

$$\boldsymbol{NOT} := \begin{bmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{bmatrix}, \quad \boldsymbol{NOT}(|\boldsymbol{A}\rangle) = \begin{bmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{bmatrix} = \begin{bmatrix} \mathbf{0} * \boldsymbol{x} + \mathbf{1} * \boldsymbol{y} \\ \mathbf{1} * \boldsymbol{x} + \mathbf{0} * \boldsymbol{y} \end{bmatrix} = \begin{bmatrix} \boldsymbol{y} \\ \boldsymbol{x} \end{bmatrix} = |\boldsymbol{B}\rangle$$

  The NOT gate is one of the three **Pauli gates**, known as **ROTX**. A binary version of this gate, **CNOT** (controlled NOT) flips the value of the first qubit depending on the value of the second.

$$\boldsymbol{CNOT} := \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}, \quad \boldsymbol{CNOT}(|\boldsymbol{AB}\rangle) = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \boldsymbol{w} \\ \boldsymbol{x} \\ \boldsymbol{y} \\ \boldsymbol{z} \end{bmatrix} = \begin{bmatrix} \boldsymbol{w} \\ \boldsymbol{x} \\ \boldsymbol{z} \\ \boldsymbol{y} \end{bmatrix}$$

  The CNOT gate may be applied to render two qubits in a **Bell state**.

- **Pauli Gates:** The Pauli Gates alter the relative phase and state of a qubit about the X, Y, or Z axis of the Bloch sphere depending on which gates are used. Respectively these are the ROTX (or the NOT gate), **ROTY** and **ROTZ** gates: the ROTX and ROTY alter the qubit's state about the real and complex axis, where the ROTZ gate alters the relative phase (about the imaginary axis).

$$\boldsymbol{Y} := \begin{bmatrix} \mathbf{0} & -\boldsymbol{i} \\ \boldsymbol{i} & \mathbf{0} \end{bmatrix}, \qquad \boldsymbol{Z} := \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & -\mathbf{1} \end{bmatrix}$$

  The variable φ corresponds to the angle by which the qubit's phase is to be rotated.

- **Hadamard Gate:** Considered the defining gate of quantum computing, the Hadamard Gate is responsible for rendering a qubit from a deterministic state into a superposition, a probabilistic state, and vice versa:

$$\boldsymbol{H} := \sqrt{\mathbf{2}}^{-\mathbf{1}} \begin{bmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & -\mathbf{1} \end{bmatrix}$$

  It is its own inverse: the effect imposed on a qubit is undone when the Hadamard Gate is applied an even number of times, due to the $\sqrt{2}$ coefficient.

Copying the value of a qubit is not possible when attempted during its lifetime: to copy a qubit requires one to know, definitively, its value, which requires measurement, destroying the qubit and converting it to classical information consequentially. This nature has implications for cyber security over **quantum networks**.

In classical computation operations are performed sequentially (one at a time), whereas in quantum computation operations are performed in a parallel manner (at the same time). This is achieved with the property of **quantum entanglement**, which makes quantum computing naturally concurrent. Entanglement is only observable in systems of multiple qubits, which are said to be in a state of entanglement after their representative particles have interacted at one point in their existence. Once entangled, measuring the value of one qubit enables the values of the other(s) to be measured immediately at the same time with no latency between them regardless of their separation distance: this is known as **quantum teleportation** (QT), and constitutes the inherently parallel nature of quantum computing. Any pair of entangled qubits A and B constitutes a Bell State, which is expressed as:

$$|\boldsymbol{\phi}^{\pm}\rangle_{AB} = \left(|\mathbf{0}\rangle_{A}|\mathbf{0}\rangle_{B} \pm |\mathbf{1}\rangle_{A}|\mathbf{1}\rangle_{B}\right)/\sqrt{\mathbf{2}}$$

where $\boldsymbol{\phi}^{\pm}$ corresponds to the angle of the relative phase shared between the qubits. There are various advantages inherent with quantum parallelism, such as reducing the time complexities of algorithms, and heightened energy efficiency, although this supremacy can come at a cost of consistency caused by a phenomenon referred to as **quantum noise**, which arises from uncertainties in the amplitude and phase associated with a quantum state due to external interference.

2 Applied quantum networks

2.1 Quantum networking

The field of **quantum networking** applies the characteristics of entanglement to establish connections facilitated over a mixture of classical and quantum channels to achieve greater network speeds and security between clients. **Quantum Key Distribution** (QKD) increases network safety by enabling clients to communicate consistently without the extended risk of being subject to a MITM attack, and comprises of the following process:

1. generate a new qubit using specific settings,
2. encode qubit in a superposition $|\varphi\rangle$ using the HAD gate,
3. send the qubit to a target client,
4. the recipient decodes the qubit by applying the HAD gate,
5. the clients compare their qubits,
    a. if they are identical in value, their connection is (probably) safe,
    b. if they are unidentical in value, a hacker is eavesdropping.

Qubits cannot be duplicated, thus any hacker performing a MITM attack is forced to apprehend the sender's qubit, decode it, measure (and destroy) it, then blindly attempt mimicking it, ignorant of the sender's settings. Whenever there is a MITM attack being conducted on a QKD network there exists the probability of the hacker being detected: a single qubit is required to achieve this, wherein clients can react before enough qubits constituting meaningful data are exchanged. The QKD paradigm was standardized in 1984 by researchers Charles Bennet and Gilles Brassard (Bennett, Brassard, 1984, pp.175), and has since been referred to as the BB84 protocol.

Quantum Secure Direct Communication (QSDC) was proposed in 2002 (Long, Liu, 2002) as an alternative to the BB84 protocol, bypassing any application of the HAD gate for encryption. QSDC involves the direct transmission of information between the peers of a network via the following process (Qi, et al., 2019, pp.2):

1. generate a sequence of qubits in random states,
2. send one qubit to a target client,
3. the recipient measures the qubit,
4. the recipient communicates the measurement with the sender,
5. the clients compare parity of measurements to assess the security of their connection,

6. the recipient applies a cipher to the remaining information and shares it with the sender,
7. the sender decodes the remaining information using the cipher.

Rather than each qubit being transmitted in a superposition, it is transmitted in a deterministic eigenstate (for example, $|0\rangle$ or $|1\rangle$), relying on a classical channel for encryption.

QT extinguishes latency between clients, wherein a network can be facilitated with the use of at least three qubits:

- one for the sender (A),
- one for the receiver (B),
- one for their connection (C).

From here, quantum entanglement can be applied to achieve an inferred connection between qubits A and B through qubit C. By having qubits B and C interact a state of entanglement will exist between them, then by subsequently entangling A and C an inferred connection will be established between A and B. After the sender alters their qubit "A" a corresponding state will be imposed on B (the receiver) through the connection C. Upon measuring the value or altering the superposition of A, qubits B and C, too, will be measured/altered via a chain reaction: from the measured/altered value of B, the receiver can determine the message which A sent them. This phenomenon is instantaneous and inaccessible by non-clients, implying that through this quantum network, clients can communicate with zero latency and zero risk. However, for entangled qubits to be shared between clients a classical channel is required to propagate them. This implies that latency can still be an issue, albeit not due to the quantum channel.

2.2 Applied quantum teleportation

A proposal by European scientists reported in a paper titled *CubeSat quantum communications mission* (Oi, et al., 2017) suggests that implementations and advancements in quantum networks could be facilitated with CubeSat (nanosatellite) technology. They present a design for an orbit-to-ground quantum communications network for both QT and QKD using the CubeSat paradigm, which may be deployed from the International Space Station (ISS). As part of the paper's discussion, the QUESS (Quantum Experiments at Space Scale) satellite (also referred to as "Micius") – a 600kg, Sun-synchronous nanosatellite launched in 2016 by the China National Space Agency – is revered as a successful and experimentally meaningful example of how CubeSat technology can be used to facilitate quantum communications (Oi, et al., 2017, pp.1-2).

An experiment conducted with Micius by Chinese computer scientists during the same year (Ren, et al., 2017, pp.70) saw the application of three photons (whose quantum states each constitute a single qubit) in the transmission of a superposition belonging to the first photon ($\mathbf{p_1}$), denoted mathematically as:

$$\boldsymbol{|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1}$$

generated at a ground station situated in Ngari, Tibet approximately 5km above sea level. The superposition was teleported to Micius while it orbited Earth at displacements between 500km and $1{,}400\text{km}$ from the Ngari ground station. The second photon ($\mathbf{p_2}$) accompanies the first at Ngari, where the third photon ($\mathbf{p_3}$) is transmitted via a classical channel to Micius after establishing a Bell state with $\mathbf{p_2}$, expressed as:

$$|\boldsymbol{\phi}^{+}\rangle_{\mathbf{23}} = \left(|\mathbf{0}\rangle_{\mathbf{2}}|\mathbf{0}\rangle_{\mathbf{3}} + |\mathbf{1}\rangle_{\mathbf{2}}|\mathbf{1}\rangle_{\mathbf{3}}\right)/\sqrt{\mathbf{2}}$$

$\mathbf{p_1}$ constitutes the quantum channel connecting $\mathbf{p_2}$ and $\mathbf{p_3}$, wherein a measurement of $\mathbf{p_1}$ causes a measurement of $\mathbf{p_2}$, and a teleportation of a corresponding state to $\mathbf{p_3}$, which varies based on this measurement. Four possible Bell States constitute the network:

1. $|\boldsymbol{\phi}^{+}\rangle_{\mathbf{12}} = \left(|\mathbf{0}\rangle_{\mathbf{1}}|\mathbf{0}\rangle_{\mathbf{2}} + |\mathbf{1}\rangle_{\mathbf{1}}|\mathbf{1}\rangle_{\mathbf{2}}\right)/\sqrt{\mathbf{2}}$
2. $|\boldsymbol{\phi}^{-}\rangle_{\mathbf{12}} = \left(|\mathbf{0}\rangle_{\mathbf{1}}|\mathbf{0}\rangle_{\mathbf{2}} - |\mathbf{1}\rangle_{\mathbf{1}}|\mathbf{1}\rangle_{\mathbf{2}}\right)/\sqrt{\mathbf{2}}$
3. $|\boldsymbol{\phi}^{+}\rangle_{\mathbf{23}} = \left(|\mathbf{0}\rangle_{\mathbf{2}}|\mathbf{0}\rangle_{\mathbf{3}} + |\mathbf{1}\rangle_{\mathbf{2}}|\mathbf{1}\rangle_{\mathbf{3}}\right)/\sqrt{\mathbf{2}}$
4. $|\boldsymbol{\phi}^{-}\rangle_{\mathbf{23}} = \left(|\mathbf{0}\rangle_{\mathbf{2}}|\mathbf{0}\rangle_{\mathbf{3}} - |\mathbf{1}\rangle_{\mathbf{2}}|\mathbf{1}\rangle_{\mathbf{3}}\right)/\sqrt{\mathbf{2}}$

if $|\boldsymbol{\phi}^{+}\rangle_{\mathbf{12}}$ is applied $\mathbf{p_3}$ will carry a desired state, or the identical state to $\mathbf{p_1}$ for an application of $|\boldsymbol{\phi}^{-}\rangle_{\mathbf{12}}$.

The experiment demonstrated the viability of applying QT in network communications, where teleported states can be probabilistically selected via manipulating the phase angles of the qubits constituting a quantum channel.

2.3 The quantum internet

In the paper *When entanglement Meets Classical Communications: Quantum Teleportation for the Quantum Internet* (Cacciapuoti, et al., 2020) the notion of the **quantum internet** – a hypothesised successor to the modern internet applying principals of quantum networking for heightened performance and security – is discussed, including the implementation (and limitations) of QT.

Experiments were conducted using the IBM Q quantum processor, wherein it was shown that while communication using QT occurs over relatively short distances (with the experiment conducted by the Chinese scientists (Ren, et al., 2017) being a notable exception), QT serves as a centrepiece to the viable implementation of a quantum internet.

2.4 Applied quantum key distribution

A subsequent experiment (to that conducted by Ren, et al., 2017) also conducted by Chinese scientists in 2021 (Chen, et al., 2021 pp.214) demonstrated an application of QKD to networks facilitating online banking in metropolitan areas in China. The experiment involved an integrated space-to-ground communication network comprising of six constituent networks: Beijing, Hefei, Jinan, Shanghai, Nanshan, and Xinglong.

Collectively, these networks provided a ground range of $2{,}000\text{km}$, and a ground-to-air range of $2{,}600\text{km}$, equating to a total peer-to-peer range of $4{,}600\text{km}$. The Beijing network's architecture is contained within an administrative complex, consisting of five layers:

1. application layer,
2. classical logical layer (software),
3. classical physical layer (hardware),
4. quantum logical layer (software),
5. quantum physical layer (hardware).

The classical layer first checks if a user's message possesses a valid (safe) key, and if not, the quantum layer is employed to generate a new (safer) key for the message. Nanshan and Xinglong ground stations are each connected to quantum satellites (one being the Micius satellite from the preceding experiment by Ren, et al., 2017) and constitute the backbone of the network.

The Beijing, Shanghai, Hefei, and Jinan ground stations constitute the metropolitan section of the network, capable of hosting 150 users at a time.

It was reported in the paper that, over the course of the research, a resistance to several attacks (see table 1) on the quantum network had been demonstrated (Chen, et al., 2021, pp.218).

Table 1. Breakdown of the types of cyber-attack observed throughout the quantum metropolitan network.

Attack	Description
Photon-number-splitting	A hardware-oriented issue which causes the sender to produce a surplus of photons containing identical data, which can be apprehended by a spy, who may then send one of them to the receiver and decrypt the remainder to uncover a quantum key without any explicit consent. This may be used as a means of bypassing the risk of detection during a MITM attack.
Blinding	A spy manipulates a client to compute a value for them using a function which they do not know, then retains the result(s) using an encryption cypher as a means of gaining information on the function. This knowledge may be used to further assess a network's vulnerabilities for a subsequent attack.
Time-shift	A spy intercepts quantum information via a MITM attack, then attempts to remain inconspicuous by exploiting the minute inaccuracies of quantum networks by altering the time at which the information reaches the recipient based on the classical value they measure from the intercepted qubit. Such an attack was first proposed in the paper *Time-Shift Attack in Practical Quantum Cryptosystems* (Qi, et al., 2006).
Wavelength-dependency	A hardware-related issue arising from a quantum computer's beam splitter (BS) array[1]. A spy may use intercepted qubits as a reference for mimicking the BS settings applied by a sender, which can then be used for inconspicuously mimicking the information and remaining undetected.
Trojan-horse	A user downloads and/or runs a virus disguised as a trustworthy software, compromising the integrity of their system.

The research conducted in this paper demonstrated the application of the BB84 protocol in a practical.

[1] A beam splitter blocks a percentage of a beam of incident photons based on their quantum states (spin and wavelength) as a function of its angle, generating a superposition (represented by the coupling ratio of the split beams) for each qubit.

2.5 Quantum games

Experimental and proof-of-concept research conducted by Dr James Wooten demonstrated that fundamental concepts of quantum computing (superposition and entanglement) may be applied to the creation of video games (Wooten, 2017) in a meaningful way. One such game is *Quantum Awesomeness* (Wooten, 2018 (as reported by Physics World)), which is is a puzzle game created for benchmarking quantum computers. Players are presented with grids comprising of nodes (coloured dots) which contain values: blue and red dots represent low and high values, respectively. Between each node is a line connecting them, denoted by a letter. It is the player's objective to find the pairs which comprise of two identical values.

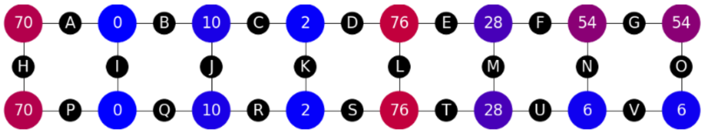

Fig. 1. Illustration of a puzzle depicted in Quantum Awesomeness (Wooten, 2018).

Quantum Awesomeness was programmed in a variety of quantum programming languages (Qiskit, Cirq, ProjectQ, and Forest) to maximize its compatibility across quantum devices, and in doing so players can run it on any quantum device (accessible via a cloud service) to see how well it performs. The game applies the concept of quantum noise as a basis for its difficulty: the less noise a quantum computer experiences, the easier Quantum Awesomeness will be for the player. Once the puzzles become too difficult for the player to solve due to the disruption caused by the quantum noise, a "game over" condition is applied.

Prior to Quantum Awesomeness, Wooten replicated the game *Battleships* using similar methods, creating *Quantum Battleships*, which he declared as the world's first (local) quantum multiplayer game (Wooten, 2017) accommodating two players.

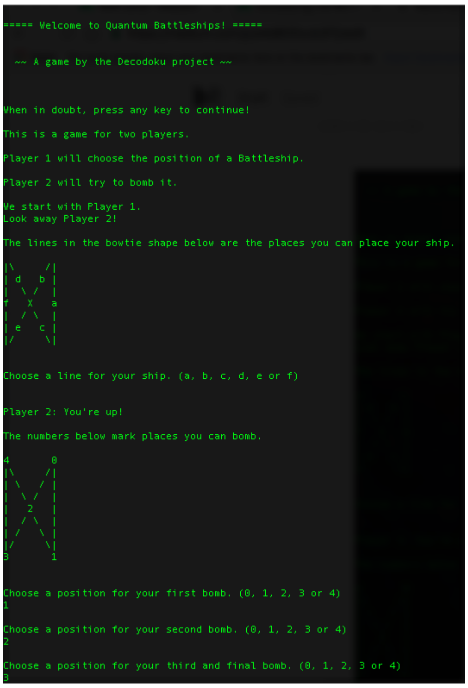

Fig. 2. Screenshot of Quantum Battleships (Wooten, 2017).

Player one (P1) is instructed to position their ship along one of seven predetermined lines (a,b,c,d,e,f), where player 2 (P2) is challenged to select vertexes on those lines where they believe P1's battleship to be located. The probability of a measuring qubit as either 0 or 1 is utilized to represent a ship's health, in place of a mutable variable. The eigenstate $|0\rangle$ represents a ship which is intact, and $|1\rangle$ represents one which has been destroyed, where their superposition $|\psi\rangle$ is used to express intermediate values (e.g., 81% health). The effects of P2's bombs are implemented with the application of a NOT gate, wherein a ship can be rendered from intact ($|0\rangle$) to destroyed ($|1\rangle$).

3 New horizons in quantum networking

3.1 Future of quantum networks for online gaming

The experiments conducted by the Chinese scientists (Qi, et al., 2017) (Ren, et al., 2017) (Chen, et al., 2021) and their experimental apparatuses demonstrate that quantum networking may be used viably to increase cyber security, with a meaningful resistance to MITM attacks and their alternatives. The next steps required in this area are to decrease the inefficiencies experienced throughout quantum networks caused by effects of noise and photon loss.

While the experiments conducted by Wooten provide a proof-of-concept demonstrating that quantum technologies may be used for implementing basic gaming software, they do not demonstrate their potential application in online gaming networks. The experimental findings of Qi, Ren, Chen, Cacciapuoti, and others collectively demonstrate this viability wherein client security (via QKD or QSDC) and communication speeds (via QT under a quantum network) may be enhanced, with the former holding more sway in this prediction due to the latter's reliance on classical channels.

Online games of the future which apply quantum networking techniques are likely to see a decrease in instances where users' personal information is taken against their wills via MITM attacks. This prediction should be acted upon with further experimental research applying QKD and QSDC protocols to rudimentary $1:1$ online multiplayer networks wherein their effects can be monitored and modified as simplistically as possible. From there, further experimental research may be conducted on online multiplayer networks featuring $1:n$ or $m:n$ client connectivity.

References

1. Benioff, P., 1980. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turning Machines. *Journal of Statistical Physics*, 22(5), pp.563-591.
2. Bennett, C.H., Brassard, G., 1984. Quantum Cryptography: Public Key Distribution and Coin Tossing. *IEEE International Conference on Computers, Systems & Signal Processing*, n/a, pp.175-179.
3. Cacciapuoti, A.S., Caleffi, M., Van Meter, R., Hanzo, L., 2020. When Entanglement Meets Classical Communications: Quantum Teleportation for the Quantum Internet. *IEEE Transactions on Communications*, 68(6), pp.3808-3833.
4. Chen, Y.A., et al., 2021. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, [PDF] 589(7841), pp.214-219. Available through: National Library of Medicine <https://www.ncbi.nlm.nih.gov/pubmed/33408416> [Accessed 22nd March 2021].
5. Harrow A.W., Montanaro, A., 2017. Quantum computational supremacy. *Nature*, [PDF] 549(7671), pp.203-209. Available through: National Library of Medicine <https://www.ncbi.nlm.nih.gov/pubmed/28905912> [Accessed 17th April 2021].
6. Hidary, J., 2019. *Quantum Computing: an applied approach*. Cham: Springer.
7. Johnston, E.R., Harrigan, N., Gimeno-Segovia, M., 2019. *Programming quantum computers: essential algorithms and code samples*. Cambridge: O'Reilly.
8. Li, H.W., et al., 2011. Attacking practical quantum key distribution system with wavelength dependent beam splitter and multi-wavelength sources. *Zhengzhou Information Science and Technology Institute*, [PDF] 84(6), pp.1-5. Available through: American Physical Society (APS) <https://dx.doi.org/10.1103/physreva.84.062308> [Accessed 9th May 2021].
9. Long, G.L., Liu, X.S., 2002. Theoretical efficient high-capacity Quantum Key Distribution Scheme. *Physical Review A*, [PDF] 65(3), n/a. Available through: American Physical Society (APS) <https://dx.doi.org/10.1103/physreva.65.032302> [Accessed 9th May 2021].
10. Medium, Wooten, J., 2017. *Quantum Battleships: The first multiplayer game for a quantum computer*. [online] Available at: <https://decodoku.medium.com/quantum-battleships-the-first-multiplayer-game-for-a-quantum-computer-e4d600ccb3f3> [Accessed 20th April 2021].
11. Medium, Wooten, J., 2018. *Using a simple puzzle game to benchmark quantum computers*. [online] Available at: <https://decodoku.medium.com/understanding-quantum-computers-through-a-simple-puzzle-game-a290dde89fb2> [Accessed 10th May 2021].
12. Oi, D.K.L., et al., 2017. CubeSat quantum communications mission. *EPJ Quantum Technology*, [PDF] 4(1), pp.1-20. Available through: SpringerOpen < https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-017-0060-1> [Accessed 3rd March 2021].
13. Physics World, 2018. *Playing games with quantum computers*. [online] Available at: <https://physicsworld.com/a/game-on/> [Accessed 20th April 2021].
14. Qi, B., Fung, F.C.H., Lo, H.K., Ma, X., 2006. Time-Shift Attack in Practical Quantum Cryptosystems. *Center for Quantum Information and Quantum Control (CQIQC), Dept. of Physics and*

Dept. of Electrical and Computer Engineering, University of Toronto, [PDF] 7(1,2), pp.73-82. Available through: Rinton Press <https://dx.doi.org/10.26421/qic7.1-2-3> [Accessed 9th May 2021].

15. Qi, R., et al., 2019. Implementation and security analysis of practical quantum secure direct communication. *Springer Science and Business Media LLC*, [PDF] n/a, 8(1). Available through: Light: Science & Applications <https://dx.doi.org/10.1038/s41377-019-0132-3> [Accessed 9th May 2021].
16. Ren, J.G., et al., 2017. Ground-to-satellite quantum teleportation. *Nature*, [PDF] 549(7670), pp.70-73. Available through: National Library of Medicine <https://www.ncbi.nlm.nih.gov/pubmed/28825708> [Accessed 22nd March 2021].
17. Scherer, W., 2019. *Mathematics of quantum computing: an introduction.* Cham: Springer.
18. UKEssays. 2018. *Suitable Network To Implement In Gaming Centre Computer Science Essay.* [online]. Available at: <https://www.ukessays.com/essays/computer-science/suitable-network-to-implement-in-gaming-centre-computer-science-essay.php?vref=1> [Accessed 5 May 2021].