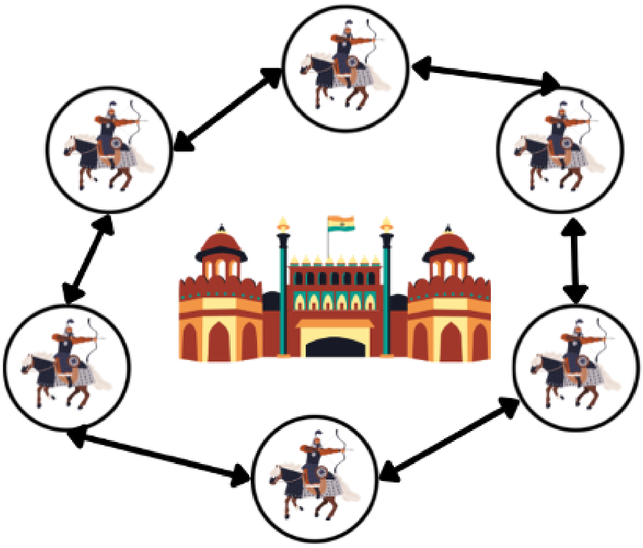
Byzantine betrayals and quantum generals

Candidate 25370

Once upon a time, byzantine armies surrounded a grand city, ready to conquer it. Each battalion, led by a powerful byzantine general was charged of maintaining siege and attacking the city from a different strategical position. Due to the grand scale of the city, these positions were spread far and wide, forcing generals to rely on messengers for coordination and communication. Yet, treachery was afoot, and each general had been warned that amongst them, lied a traitor. Fortunately, Byzantine has a very big budget and had invited time-travel a few years ago, therefore they were able to capture three wizards (nowadays knows as mathematicians) to help them find the traitor, before commencing their invasion. Leslie Lamport, Robert Shostak, and Marshall Pease, three Stanford researchers, were chosen as their wizards, and taken from their homes in the summer of 1982 to work under the Byzantine empire with the hopes to be returned to their homes and given rights to share their work with their contemporaries [1], were the siege of the city be successful.

Unfamiliar with the intricacies of Byzantine invasions, our three wizards decided to abstract this problem beyond the realms of 5th century empire conundrums. In their eyes, they were facing a networking problem.

The field of networking is a crucial aspect of communication technologies. Networks consist of a series of device connections utilized to share resources. They come in many forms, the internet, VPNs, LANs (local area networks), or time travelling byzantine generals posted outside a city. Efficient communication through a network ensures a reliable and timely exchange of information from one point to another, a requirement for the modern internet user and our 5th century invaders alike.



There are various challenges that one must overcome to ensure a strong connection:

· **Timeliness**: after all, byzantine generals can only be so patient before they start looking for a new trio of wizards. If messages are not received across the army withing a reasonable time, generals will grow tired.

· **Decentralization**: each general has its own perspective and information about the situation. Coordinating these dispersed entities to reach a unified decision is a complex task, especially when one of them may behave maliciously.

· **Communication Challenges**: even if a message is sent, our wizards have no guarantee that these messages will arrive to the receiver in their initial form. Our traitor may intercept our message, as when a message is sent between generals our messenger will stop at any other general post in its journey to feed its horse and rest.

· **Trustworthiness**: one of our generals is a traitor, and therefore we must assume that at least one of our generals will send incorrect information. Our solution needs to account for the possibility of dishonest messages.

Our trio quickly realized that solving the Byzantine Generals' Problem was in many ways analogous to solving the fundamental problems of distributed systems.

The Byzantine problem represents the major challenges in distributed computing, requiring an algorithm to reach a consensus and ensure reliable communication in the presence of faulty or malicious actors. Since the return of Leslie, Robert and Marshall, many have attempted to find the optimal solution to this problem [2-4]. Yet as of 2023, no consensus has been reached.

In the quest for more secure and resilient distributed systems, researchers are now exploring quantum networks to tackle the Byzantine general problem.

Unlike classical networks, where information is transmitted through a series of zeros and ones, quantum networks leverage qubits. Qubits are the fundamental units of quantum information utilized across various quantum technologies. From photons to diamonds, the nature of qubits is varied, yet they all adhere to the principles of quantum mechanics.

One such principle is quantum entanglement, a unique phenomenon where qubits can become correlated in ways not possible in classical systems. When two qubits are entangled, they start influencing each other, allowing us to obtain information from both qubits while observing only one. This pairing is distance-independent.

Entanglement allows for secure communication protocols based on quantum key distribution (QKD).

QKD comes in many forms, the BB84 [5] protocol is probably its most illustrative example. It works as follows:

1. One of our generals (Alice the great) prepares qubits utilizing a random basis.

   Basis serve as languages in quantum mechanics. They establish the rules for information interpreting. If one reads information in a foreign language they won't understand it, therefore shared basis are key in order to find a common understanding. BB84 uses 2 basis: rectilinear and diagonal.

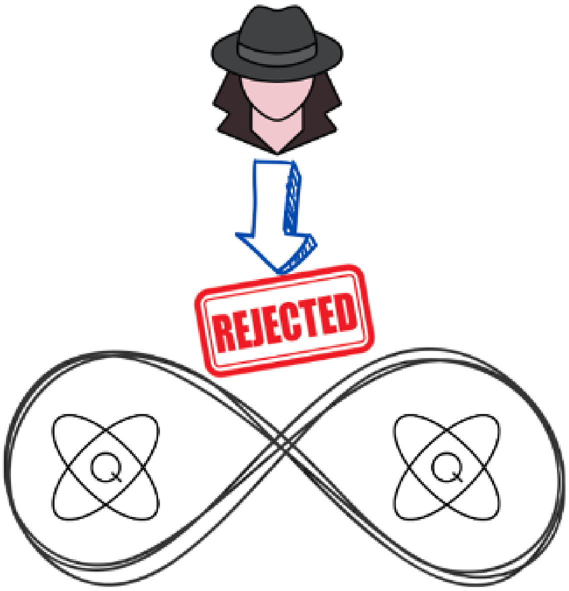
2. Another general (Bob the patient) then measures all these qubits with a separately randomly chosen basis.

3. Alice then let's Bob know what she initially created via a separate communication channel.

4. When Alices' and Bob's results coincide (which happens about 50% of the time), their shared result is added to the shared secret key between both.

5. Once they iterate through all the states Alice prepared, they finish their process and now share a secret key that safeguards them from tampering. If the traitor were to intercept their code, they would not be aware of the key-based encoding and will make noticeable errors that Alice and Bob will be able to spot as they don't respect their shared code. Thus, alerting them of malicious attempts.

QKD process protect quantum channels from being tampered with, thus allowing us to simplify our Byzantine problem, as this possible malicious tampering is no longer in the picture. Now we can now focus on devising a good game of “Simon says” to find our traitor.



Researchers, Michael Ben-Or and Avinatan Hassidim were some of the first ones to tackle the byzantine problem utilizing quantum networking principles [6]. Their byzantine quantum protocol could tolerate up to 1/3 of the generals being traitors, and still successfully sedge the city. By utilizing the properties of qubits, active research [7-8] on quantum solutions could lay the foundations of future network security.

Resources:

1. https://lamport.azurewebsites.net/pubs/byz.pdf
2. https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=BA568F344CF728CF8B35A81DBEF3A8BB?doi=10.1.1.406.3304&rep=rep1&type=pdf
3. https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Distributed%20Computation/An%20Optimal%20Probabilistic%20Algorithm%20for%20Byzantine%20Agreement.pdf
4. https://dl.acm.org/doi/pdf/10.1145/167088.167105
5. http://www2.lns.mit.edu/~avinatan/research/byzant.pdf
6. https://web.archive.org/web/20200130165639/http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf
7. https://link.springer.com/article/10.1007/s11128-022-03492-y
8. https://www.mdpi.com/2076-3417/13/14/8405