Quantum Computers and Cryptography

Imran H Shaheem

Who Am I?

- MSc in Gravity, Particles and Fields from The University Of Nottingham.
- During my studies I participated in online bug bounty programs. I found a P2 in a fortune 10 company and was part of the group awarded the 'BugCrowd 2017 VIP researcher' accolade.
- I joined Cyberis in January 2018 as a Security Consultant and began officially working in the industry.

cyberis

Quantum Information & Cryptography – The CliffsNotes

- Classical information theory originates from Shannon's 1948 paper.
- Quantum information begins with the idea that quantum systems are the ultimate physical medium for storing and processing information.
- In quantum cryptography, one would like to transmit or share information securely, using the fact that quantum states cannot be learned without being disturbed.

cyberis

Quantum Computers

Classical Computers

- Information is stored in bits, 1 and 0, if storing one number takes 64 bits then storing *n* numbers takes 64*n* bits.

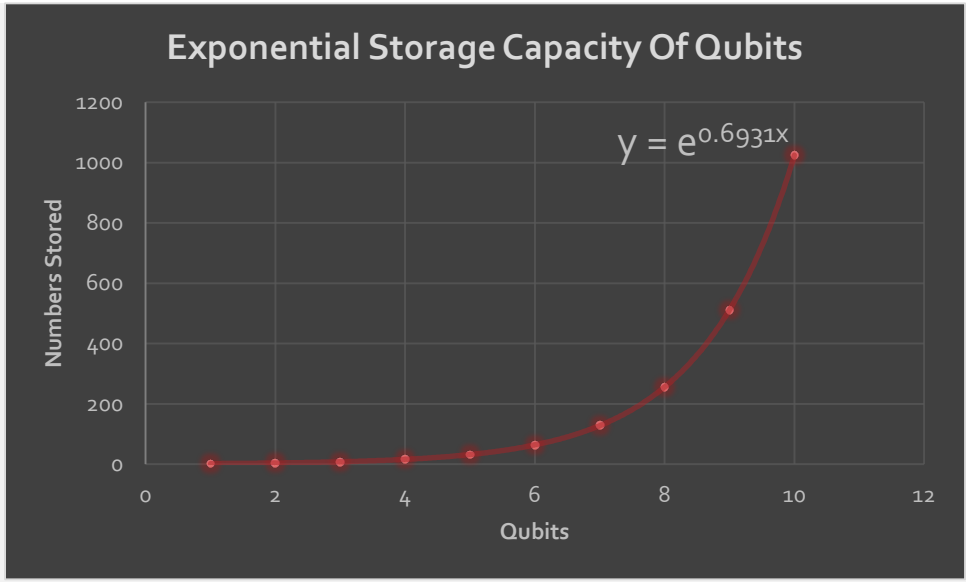
Quantum Computers

- Information is stored in quantum bits (qubits), a qubit can be in state |0> and |1> HOWEVER it can also be in a superposition of these states, $a|0> + b|1>$, where *a* and *b* are complex numbers.

- This allows far more information to be stored on a qubit. For every extra qubit you get, you can store twice as many numbers.

cyberis

Qubits
-
Exponential Storage!



1 qubit:

- |0>, |1> => Store 2 numbers.

2 qubits:

- |00>,|01>,|10>,|11> => Store 4 numbers.

3 qubits:

- |000>, |001>, |010>, |100>, |110>, |011>, |101>, |111> => Store 8 numbers.

cyberis

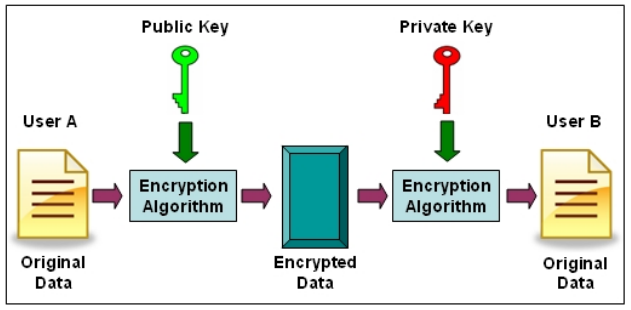
Quantum Computers - Better At Everything?

- Quantum computers utilise quantum mechanics to solve certain problems much faster than is possible with a classical computer. Quantum mechanics relies on the principles of probability.

- In general, problems that can utilise parallelism (the ability to split a problem into several parts and solve them all simultaneously to arrive at a solution) are the problems that will benefit from the gains quantum computers offer.

cyberis

Classical Cryptography - A Brief Recap



Goal: Allow secure communication of secret messages over public channels.

- One-time pad algorithm.
- Public-private key pair.

The RSA algorithm, for example, relies on the difficulty of factoring large numbers.

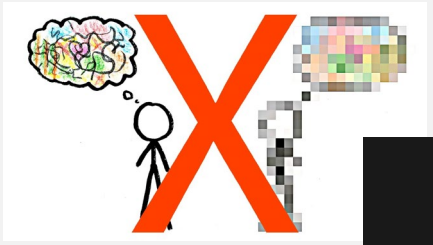
- Current computers: largest number factored ~ 250 decimal digits.
- Quantum computers: factor large numbers in polynomial time.

cyberis

Quantum Cryptography

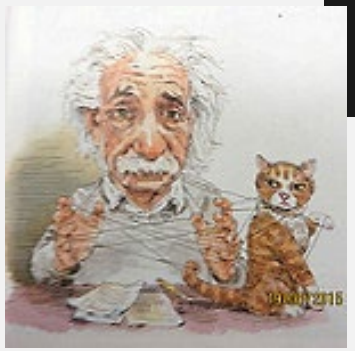
Quantum Cryptography derives its strength from a few weird properties of quantum mechanics:

- **The no cloning theorem**



- **Quantum superposition**

- **Quantum entanglement**



Quantum Cryptography – Pros and Cons

Pros:

- Cannot be unknowingly intercepted
- Secure - irrespective of computing power
- Secure communications at a physical level

Cons:

- Expensive
- Requires independent infrastructure
- Practical problems in implementation

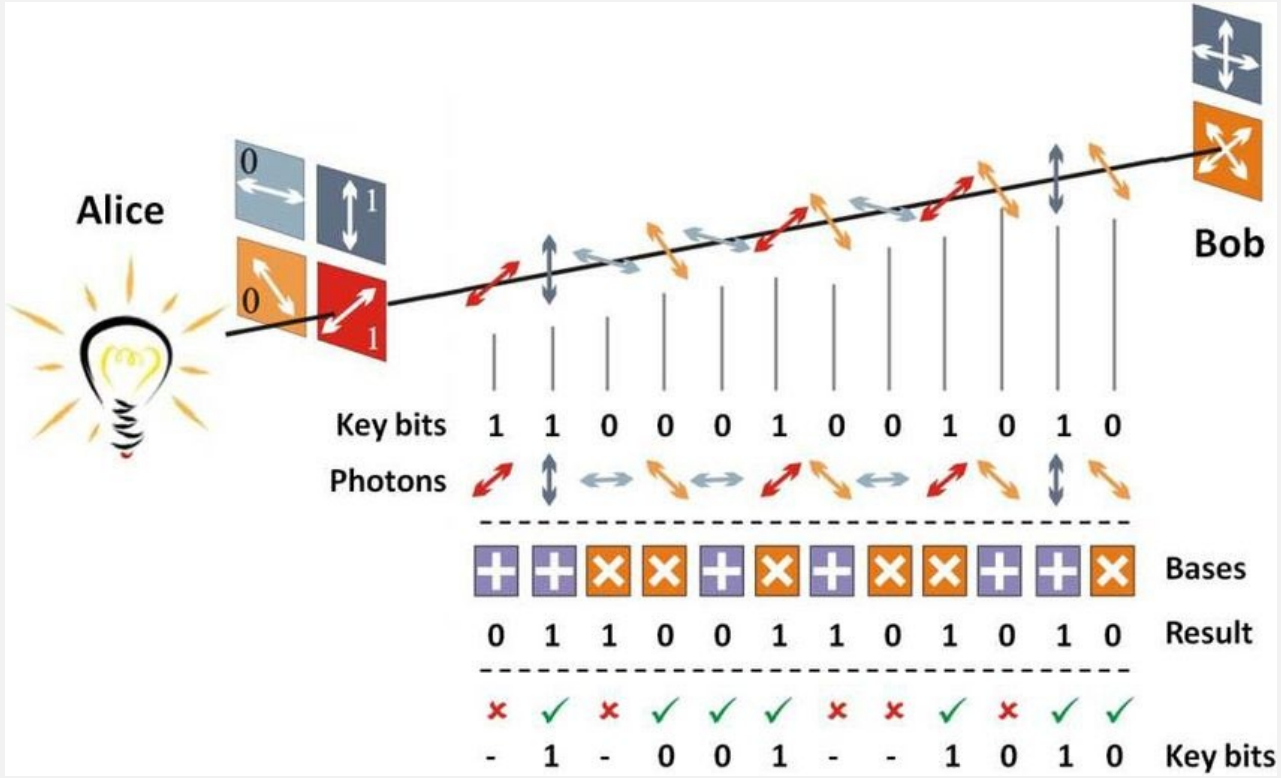
cyberis

Quantum Key Distribution – The BB84 Protocol

- **Goal:** To establish a key between Alice and Bob, such that an eavesdropper, Eve, cannot learn it by listening to their "conversation".
- The basic idea is that Alice and Bob use quantum systems to establish the key, and if Eve tries to learn the state of the system this will inevitably disturb the state, which can be detected by Alice and Bob.
- BB84 is a key distribution system proposed by Bennet and Brassard in 1984.

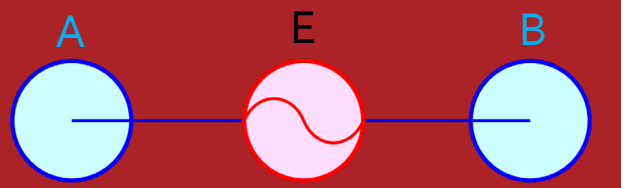
cyberis

The Steps of the BB84 Protocol



The BB84 steps. Each column represents one round of the protocol.

Security of the BB84 protocol



Is the protocol secure against an eavesdropper?

- The central principle is that in order for Eve to learn the key, the qubits sent by Alice must be intercepted and measured.
- If Eve knows the basis to which the prepared state belongs, she could measure the state in that basis and learn the state without altering it.
- However, Eve doesn't know which basis has been used, as such she can't perform the above measurement. This leaves two possible alternatives…

cyberis

Eve's First Option

Eve can choose one of the two bases randomly, measure in that basis and then pass the system on to Bob.

- If Eve chooses the same basis as that of Alice's prepared state, then she obtains the result she's looking for and can pass on the state to Bob undisturbed.
- On the other hand, if Eve measures in the other basis then the state sent to Bob will have been altered. When Bob makes his own measurement there is a 1 in 4 chance that he will obtain Alice's prepared state.

cyberis

Eve's Second Option

Eve can keep the system sent by Alice and measure it only after the classical communication declares which bases were used for encoding.

- However, she needs to send Bob a qubit prepared in a certain state, no matter what state she chooses, there is a significant chance that Bob's measurement will give a different result than the original state sent by Alice.

Some Closing Words About BB84

- In general, Eve may employ more sophisticated attacks in which several successive qubits are measured, which makes the proof of the security more complicated.

- Quantum cryptography is fast approaching the stage of technological applications, with several companies in the process of producing cryptographic systems based on the BB84 protocol.

cyberis

Penetration Testing QKD
-
Attacking BB84

"[…] what is proved by impossibility proofs is lack of imagination"

- John Stewart Bell

Loop Holes and Poor Implementation – A Pentester's playground!

- There is an assumption on almost perfect devices functioning correctly at all times to achieve "unconditional security".

cyberis

Example - The Light Injection Attack

- Eve sends light pulses towards the sender's or receiver's device, which returns as a reflected pulse.
- Eve can use the information contained within the reflected pulse to potentially learn the basis used for transmission or detection.
- Ideally, Eve manages to acquire this information before the photon reaches Bob's side, then Eve can execute a man in the middle attack without being detected.

cyberis

Securing BB84

Depending upon the physical implementation of the BB84 protocol, security measures can include:

- **Passive measures** – inherent properties of the infrastructure that make them resistant to such attacks.
- **Active measures** – the introduction of tools designed to mitigate such attacks.
- **Both** – active for Alice and passive for Bob or vice versa.

In Conclusion

- There is no better physical medium for storing and processing information than quantum systems, according to quantum information theory.
- Quantum cryptography can be secured on the physical level, there are many pros but also several cons, and physicals hurdles, yet to be overcome.
- Commercial systems relying on quantum principles are already beginning to emerge.
- While several protocols are secure in theory, there exists many pen-testing applications in the physical implementations of such systems.

cyberis

Further Reading

- **Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol** - Rahul Aggarwal, et al.
- **Breaking the Unbreakable: Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography** - Jonathan Jogenfors.
- **Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography** - Artem Vakhitov, et al.
- **Practical challenges in quantum key distribution** - Eleni Diamanti, et al.
- **Simple Proof of Security of the BB84 Quantum Key Distribution Protocol** - Peter W. Shor and John Preskill.

cyberis

Image References

- **Slide 4:** https://sites.google.com/site/apchemistryquantumcomputing/what-is
- **Slide 6:** (Adapted) Dennis Hill - https://www.flickr.com/photos/fontplaydotcom/506735407
- **Slide 7:** Mdscott - http://itlaw.wikia.com/wiki/Key_pair?file=Pke_fig1.jpg
- **Slide 8:**
  - **No Cloning Theorem:** minutephysics - https://www.youtube.com/watch?v=owPC6oUeoBE
  - **Superposition:** DezziArt - https://www.teepublic.com/mug/2160296-dead-and-alive-schrodinger-cat-funny-design-art-fo
  - **Quantum Entanglement:** Gwydion M. Williams - https://www.flickr.com/photos/45909111@N00/20853817231/
- **Slide 11:** Alberto Carrasco-Casado - (https://www.researchgate.net/figure/BB84-protocol-basic-scheme_fig11_309731586)
- **Slide 12:** (Adapted) Oseveno, Miraceti - https://commons.wikimedia.org/w/index.php?curid=60561645
- **Slide 15:** https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/

cyberis

Acknowledgements

Thanks to:

- Cyberis for allowing me the time and resources to put this presentation together.
- Mark Crowther, Kathryn Fair and Ian Londesbrough for their guidance and encouragement.
- Crest for providing such a stellar platform.
- You for listening!

cyberis