Cracking the Mystery:

Quantum Cryptography and the Future of Cybersecurity

Rajvi Khanjan Shroff

A little bit about me:

* Project Cyber Founder

* Came in at the top 3 (states rank) in Girls Go CyberStart national competition

* Started an infosec and a chess club in middle school

* Invited to ask NATO's panelist & author Ms. Nina Jankowicz a question in the "Digital Dialogue on the Gender Infodemic: Data, Disinformation and a Digital Future" event, to represent the GirlSecurity organization

How I got started + Tips:

* It's very important (and fun!) to experiment and try new things---join courses on platforms such as Coursera & Udemy that teach about the fundamentals of cybersecurity and meet other like-minded peers

* CTFs:
(CyberStart America, PICOCTF, etc)

* Read books, such as The Code Book

* Have fun!!

How to get involved in cybersecurity!

Project Cyber is an opportunity for teens to engage in conversations about digital security. Our mission is to serve as a global community for youth interested in cybersecurity.

WEBSITE: https://championing-security.postach.io/

Youtube channel: CyberMissionPossible, https://www.youtube.com/channel/UCpsskvZcPvOVnUOhEiUjD_w/featured

Instagram: https://www.instagram.com/rksmissionpossible/

Join The Team!

Teens:

Fill out the Google Form:
https://tinyurl.com/JoinProjectCyber

& Join our Google Classroom

--Submit a draft on Google Classroom, and after peer-edits, it will appear on our website!

Cybersecurity Professionals:

We're looking for those in college and beyond to be featured on
the magazine and/or be advisors!
If interested, please email at

rksmissionpossible@gmail.com

What is “quantum”?

Quantum is Latin for amount

- “The smallest discrete unit of any physical property” (such as energy or matter)

Hence, quantum mechanics is a branch of science that deals with the world on a very tiny scale (microscopic).

One application of quantum mechanics is quantum computing.

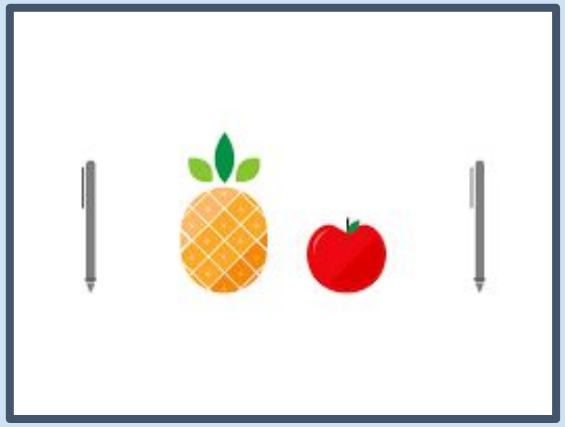
A Primer To Qubits (Quantum bits)

In computing today:
(classical computing)

→ uses bits, which are 0 **or** 1

In quantum computing:

→ uses *qu*bits, which are 0 **or** 1, **or 0 and 1 simultaneously**



Quantum Computing….
& the rise of Quantum Cryptography

- Quantum computing is much faster than classical computing --- the number of possible states qubits can be in grows exponentially, which allows a quantum computer to consider a whole lot of combinations at once.

---This makes problem-solving (e.g factoring large numbers) much quicker.

Our cryptography today is in danger, as quantum computers can break it (but classical computers cannot)-- this gives rise to *quantum* cryptography

“Types” of Quantum Cryptography

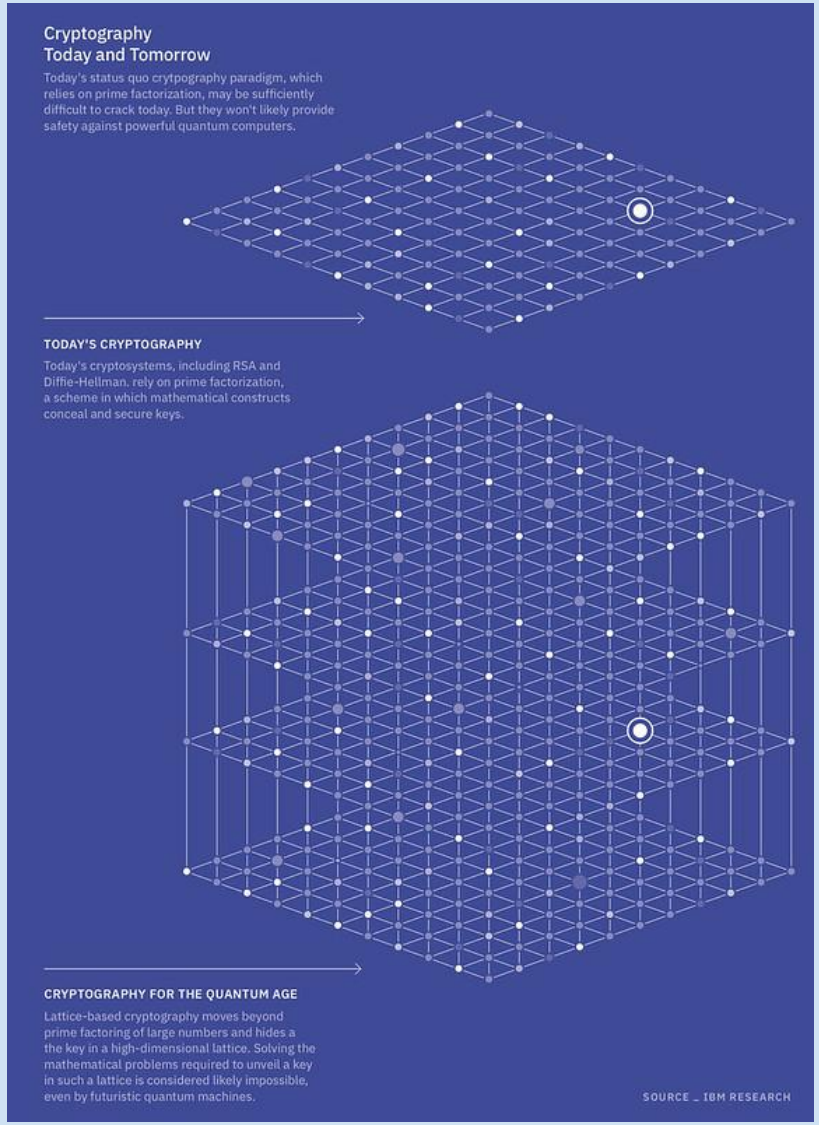
- *Post Quantum Cryptography (PQC)*

  --In particular, lattice cryptography

- *QKD (Quantum Key Distribution)*

- *Classical hybrid cryptography*

Lattice Cryptography



What lattices are:

They are a geometric grid of points that extend infinitely in all directions.

How this works:

The data is hidden in lattices, which makes for some very difficult math problems. The problem? It's quite the challenge to find two lattice points that are comparatively close together.

What that means:

This might sound simple, but experts are relying on the difficulty of solving these problems because this takes even quantum computers an incredible amount of time to unravel!

QKD (Quantum Key Distribution)

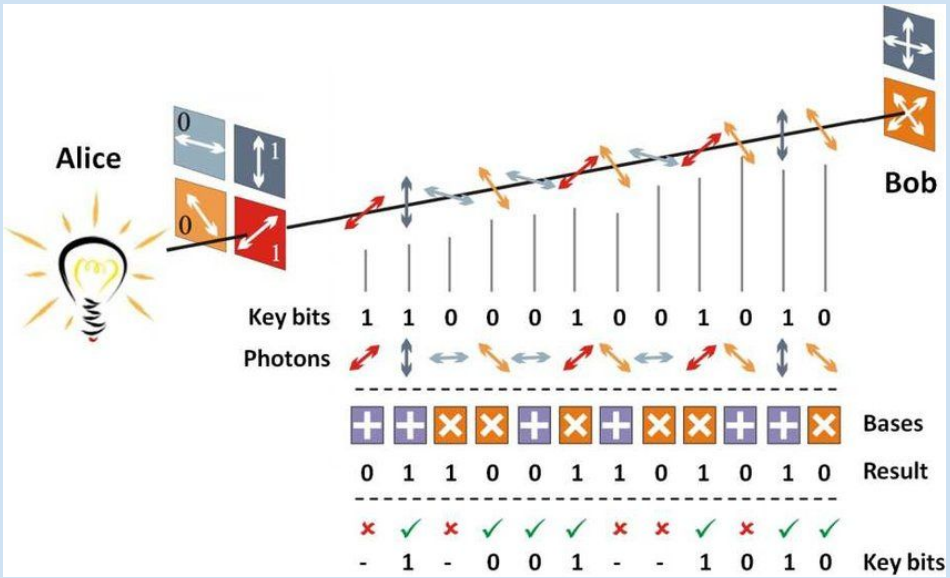
QKD is a subset of Quantum Cryptography

- It explains how a key is generated.

- One of the QKD Schemes is a BB84 Protocol. It is one of the more established ways to create keys with quantum computers.

In a nutshell, this is the process of the BB84 protocol:

There are two parties, the sender and the receiver.



Free-Space Quantum Key Distribution - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/BB84-protocol-basic-scheme_fig11_309731586 [accessed 28 Dec, 2020]

1. The sender polarizes photons in four directions and sends them to the receiver.

2. These photons are read using two detectors, meaning each photon is translated as a 0 or 1. The receiver ends up with a series of 0s and 1s, but about half of them have been read incorrectly (because the kind of detector used matters, and the receiver can only guess which one to use)

3. The receiver and sender discuss. The receiver tells the sender what filter he used for each photon.
   The sender tells the receiver if it was right or wrong.
   All photons the receiver got wrong are then discarded.

4. The photons we're left (~half of what we started) with become our key! We'll now use the key to encrypt and decrypt our messages.

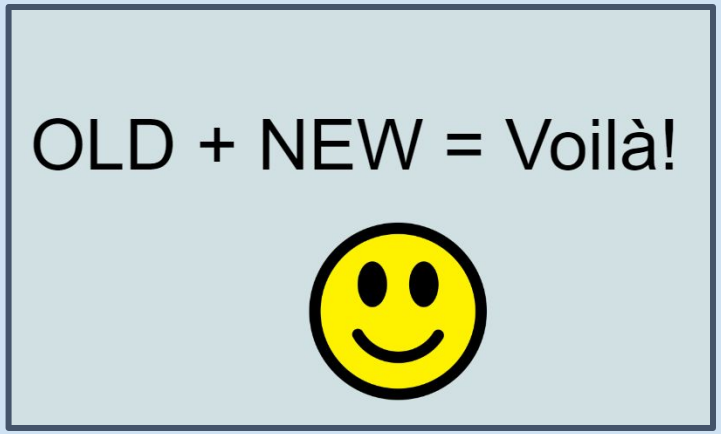
CLASSICAL HYBRID CRYPTOGRAPHY

- Uses what we have today and what we can use once quantum computers arrive, by combining the two!

  * Traditional algorithms like the RSA and ECC can be used alongside new PQC algorithms.

  * For instance, a quantum resistant algorithm such as New Hope or Sike might be used together with a classic algorithm like DHE or ECDH to generate a unique key.

To sum it up:



Looking Ahead

Research is increasing in this field and the rate of progress rising rapidly.

The word "cybersecurity" will take on a whole new new meaning!

It won’t be long until Quantum Cryptography develops as a field as rich as today’s security ecosystems

One thing's for sure: knowing the science behind quantum computing is going to be crucial, because the future is quantum.

Interested in Learning More? Resources!

Article:
https://quantum.country/qcvc

Video & Guide:
https://www.wired.com/story/wired-guide-to-quantum-computing/

Interactive Opportunity:

https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/