hackersvilla.xyz

Quantum Computing

Vs Cryptography

Presenter – Sanchay Singh
@OWASP Meetup (Online, 11 February, 2024)
and THM Delhi (Offline, 21 Jan, 2024)

hackersvilla.xyz

>_whoami

-> **Co-founder of HackersVilla CyberSecurity**

-> Security Consultant/Trainer at MakeIntern

-> Worked as SME at UpgradCampus

-> Trained Employees of KPMG, Cognizant, etc

-> Security Mentor/Speaker at OWASP Delhi

-> Security Mentor at BSides Noida

-> Active part of NULL and THM Delhi Chapter

in sanchayofficial

sanchayofficial@gmail.com

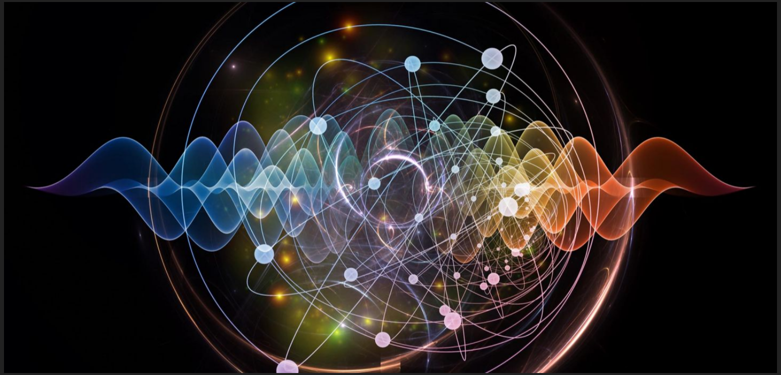
Sanchay Singh

CYBERSECURITY EXPERT | CORPORATE TRAINER | PUBLIC SPEAKER

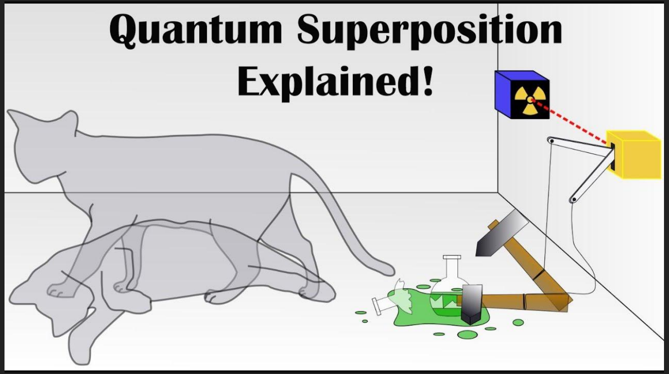
My Journey

Quantum Computing Fundamentals

Basics of Quantum Mechanics

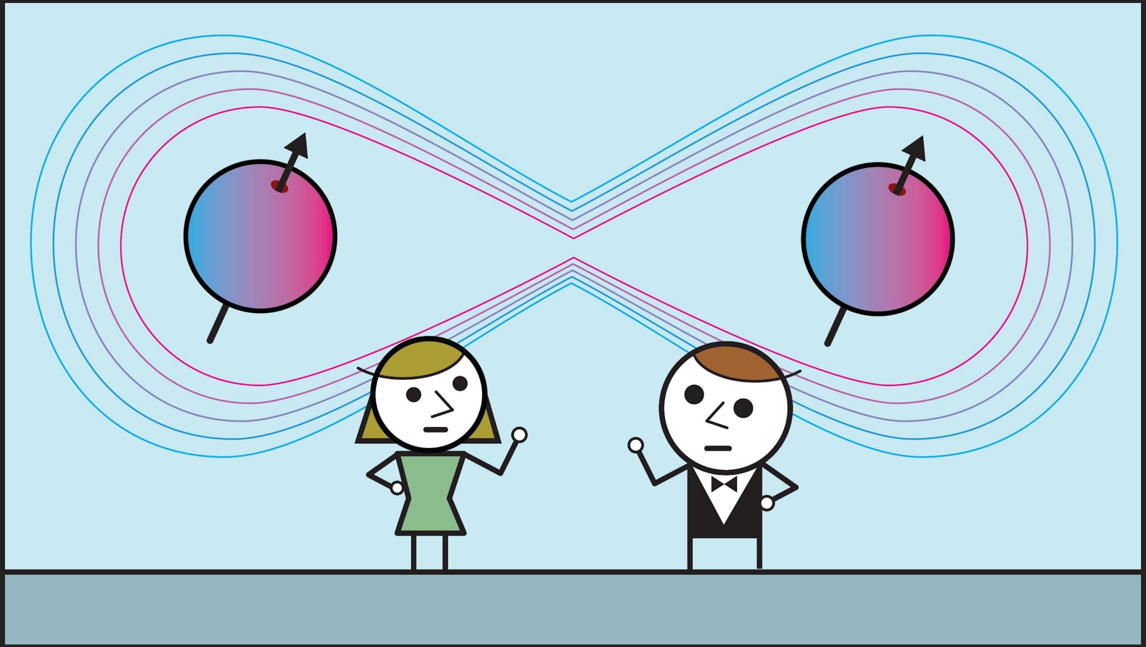


Subatomic World

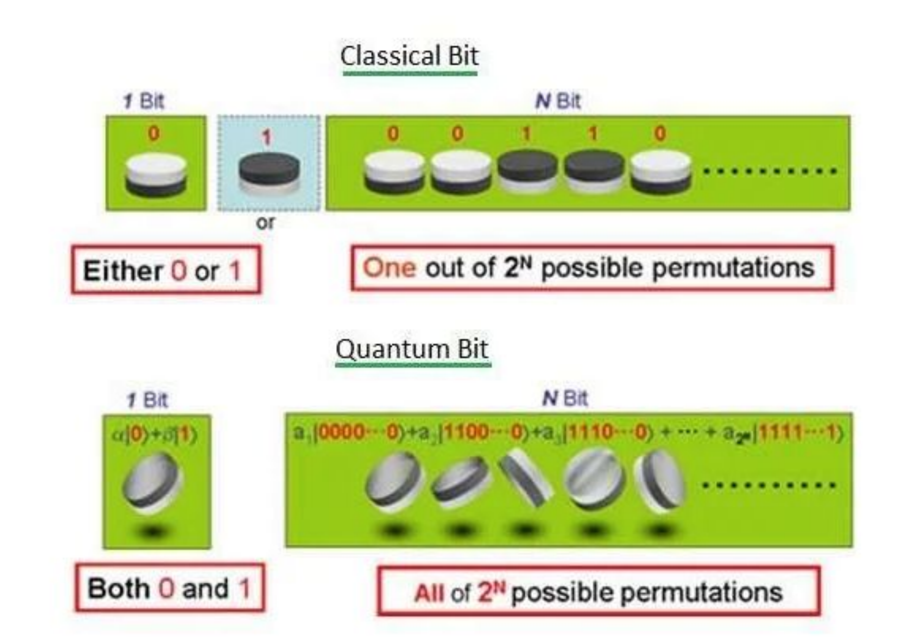


Superposition

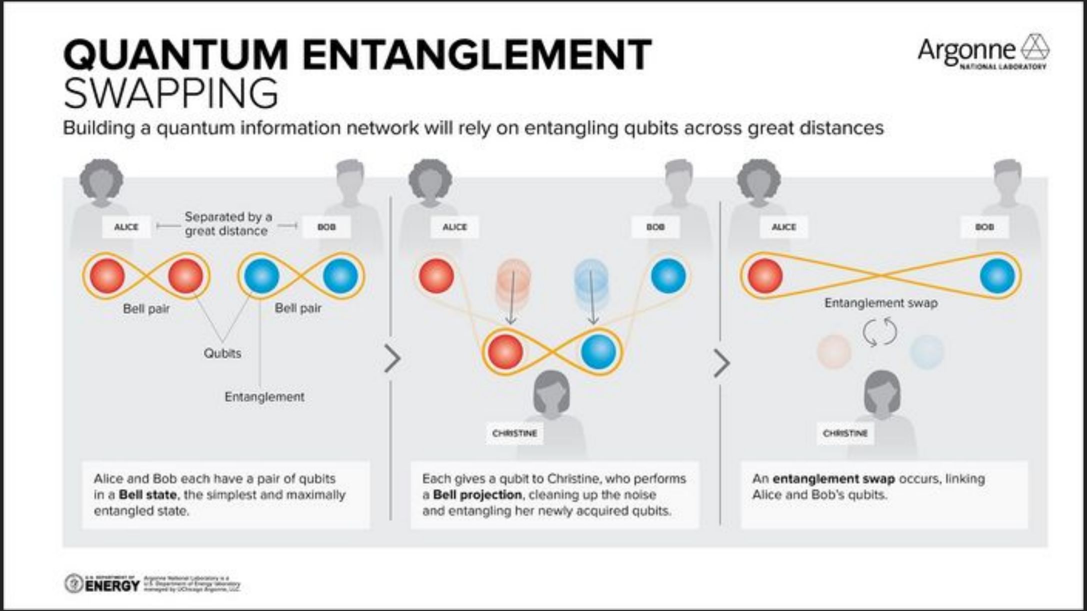
Quantum Entanglement



What are QUBITS?


Classical Bit
1 Bit
0
1
or
N Bit
0 0 1 1 0 ....
Either 0 or 1
One out of 2^N possible permutations
Quantum Bit
1 Bit
$\alpha|0\rangle+\beta|1\rangle$
N Bit
$a_1|0000\cdots0\rangle+a_2|1100\cdots0\rangle+a_3|1110\cdots0\rangle+\cdots+a_{2^N}|1111\cdots1\rangle$
....
Both 0 and 1
All of 2^N possible permutations

Let's combine them Both



QUANTUM ENTANGLEMENT
SWAPPING

Building a quantum information network will rely on entangling qubits across great distances

Alice and Bob each have a pair of qubits in a **Bell state**, the simplest and maximally entangled state.

Each gives a qubit to Christine, who performs a **Bell projection**, cleaning up the noise and entangling her newly acquired qubits.

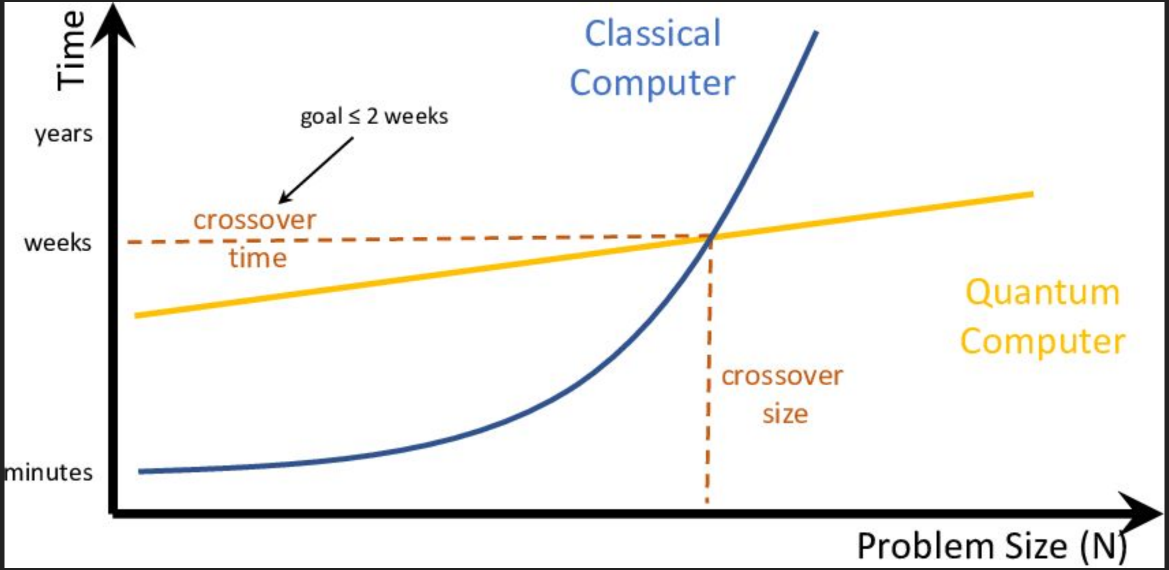
An **entanglement swap** occurs, linking Alice and Bob's qubits.

Argonne NATIONAL LABORATORY
ALICE
Separated by a great distance
BOB
Bell pair
Bell pair
Qubits
Entanglement
ALICE
BOB
CHRISTINE
ALICE
BOB
Entanglement swap
CHRISTINE
U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.

Source: https://www.eurekalert.org/news-releases/974345

hackersvilla.xyz

Quantum Speedup

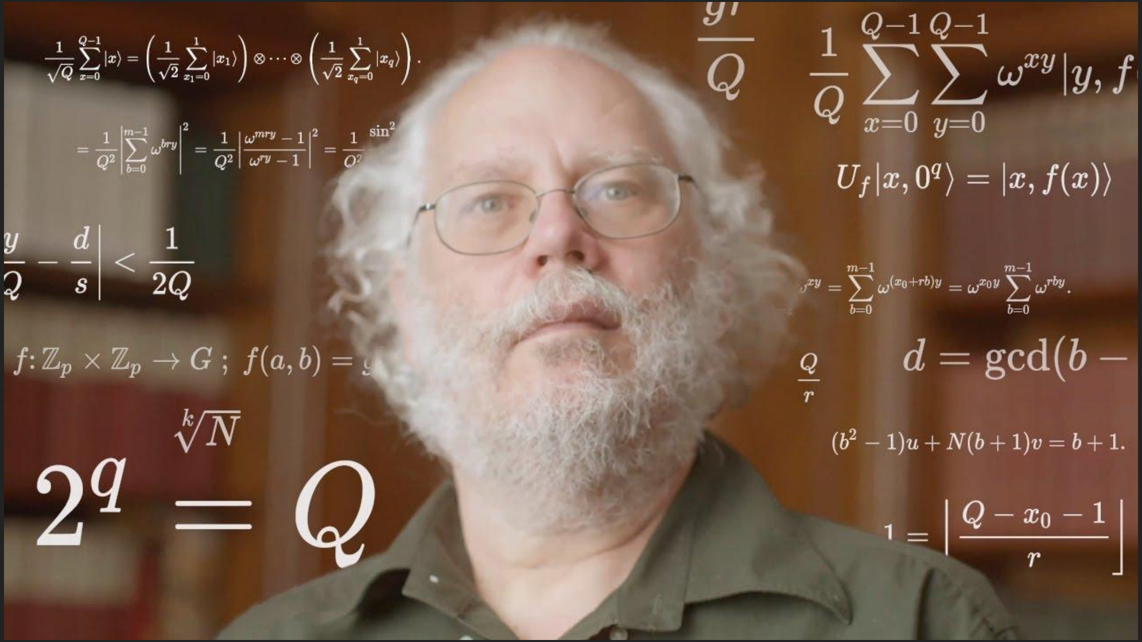


Source: https://www.researchgate.net

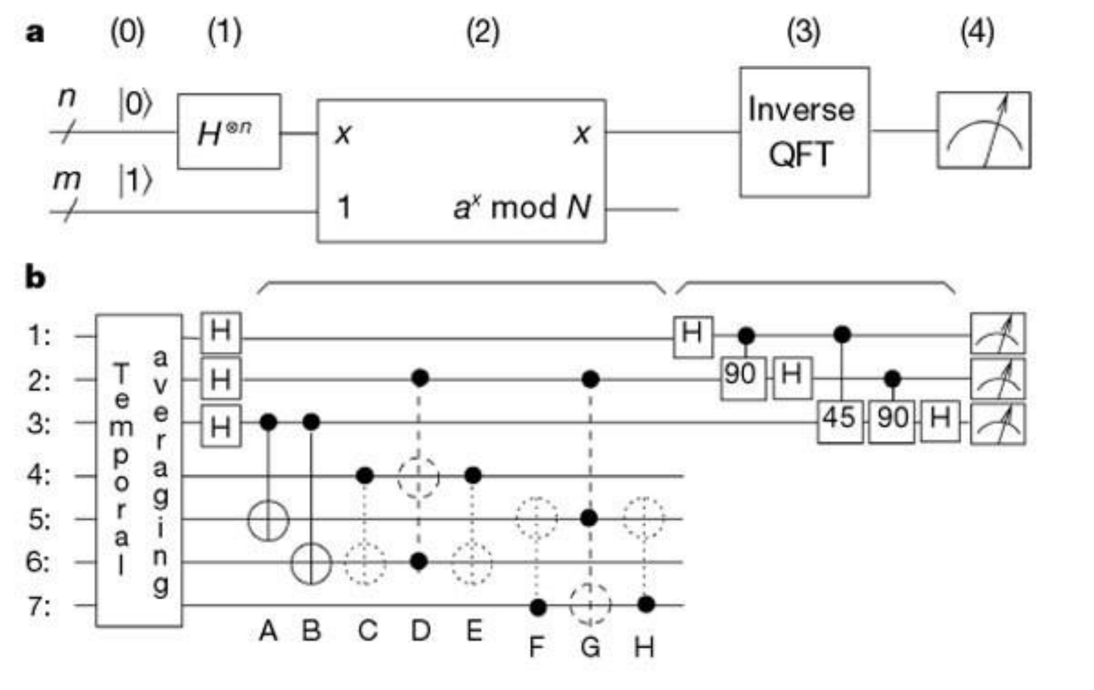
hackersvilla.xyz

Power of Quantum Computing

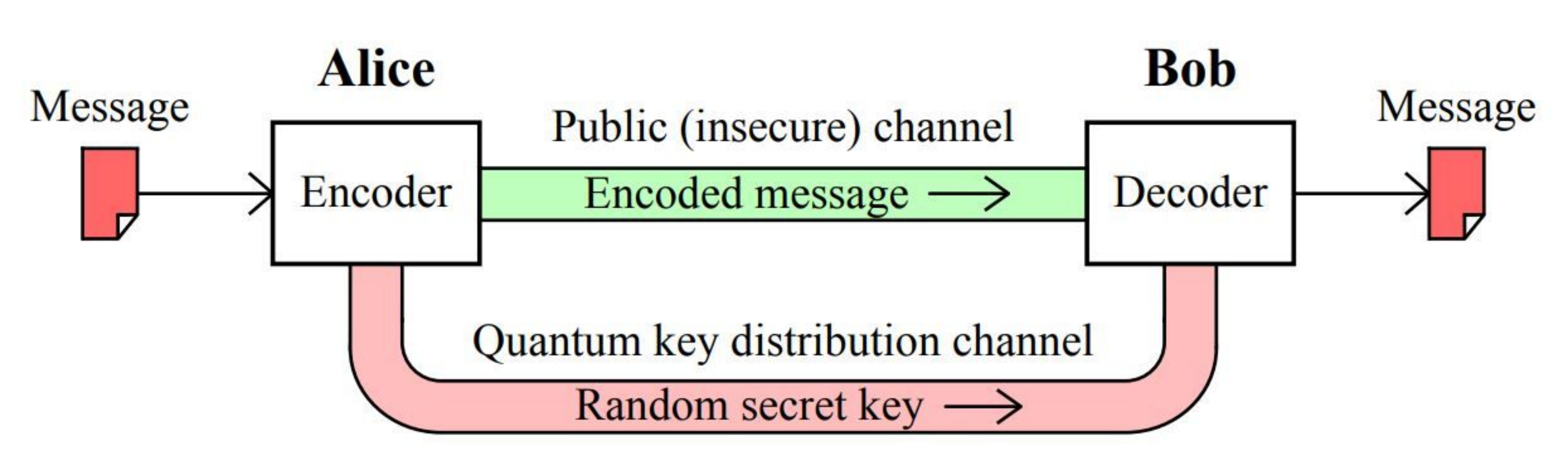
Shor's Algorithm


$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle = \left(\frac{1}{\sqrt{2}}\sum_{x_1=0}^{1}|x_1\rangle\right)\otimes\cdots\otimes\left(\frac{1}{\sqrt{2}}\sum_{x_q=0}^{1}|x_q\rangle\right).$
$= \frac{1}{Q^2}\left|\sum_{b=0}^{m-1}\omega^{bry}\right|^2 = \frac{1}{Q^2}\left|\frac{\omega^{mry}-1}{\omega^{ry}-1}\right|^2 = \frac{1}{Q^2}\sin^2$
$\left|\frac{y}{Q}-\frac{d}{s}\right| < \frac{1}{2Q}$
$f:\mathbb{Z}_p\times\mathbb{Z}_p\to G\,;\; f(a,b)=$
$\sqrt[k]{N}$
$2^q = Q$
$\frac{y}{Q}$
$\frac{1}{Q}\sum_{x=0}^{Q-1}\sum_{y=0}^{Q-1}\omega^{xy}|y, f$
$U_f|x,0^q\rangle = |x,f(x)\rangle$
$= \sum_{b=0}^{m-1}\omega^{(x_0+rb)y} = \omega^{x_0 y}\sum_{b=0}^{m-1}\omega^{rby}.$
$\frac{Q}{r}$
$d = \gcd(b -$
$(b^2-1)u + N(b+1)v = b+1.$
$1 = \left\lfloor\frac{Q-x_0-1}{r}\right\rfloor$

Shor's Algorithm

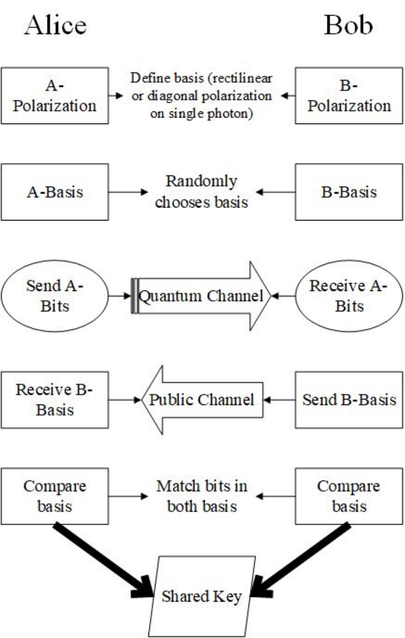


Quantum Key Distribution (QKD)



hackersvilla.xyz

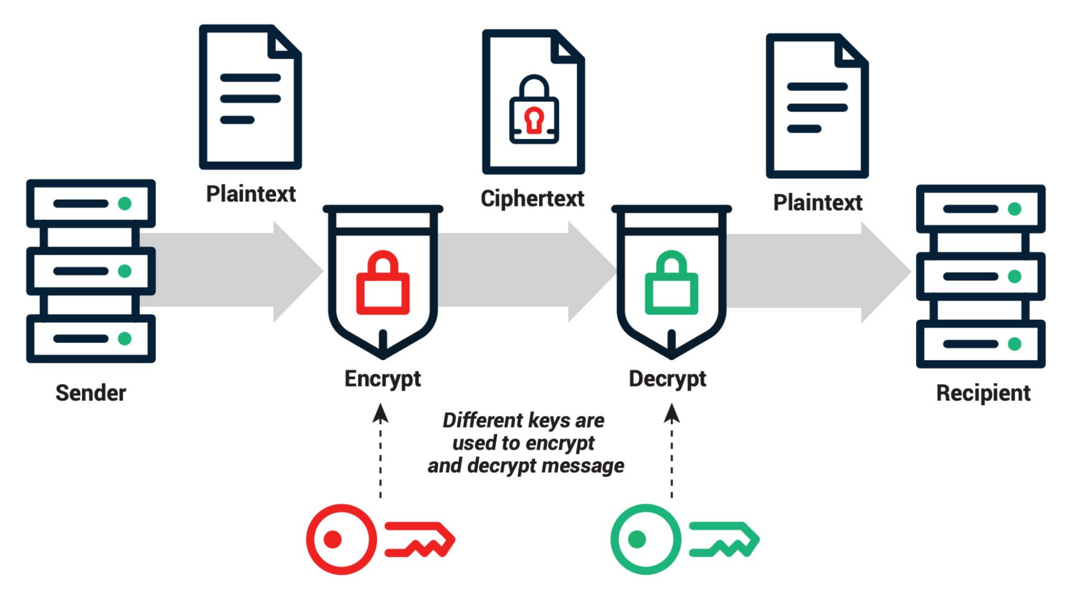
HOW QKD Works?



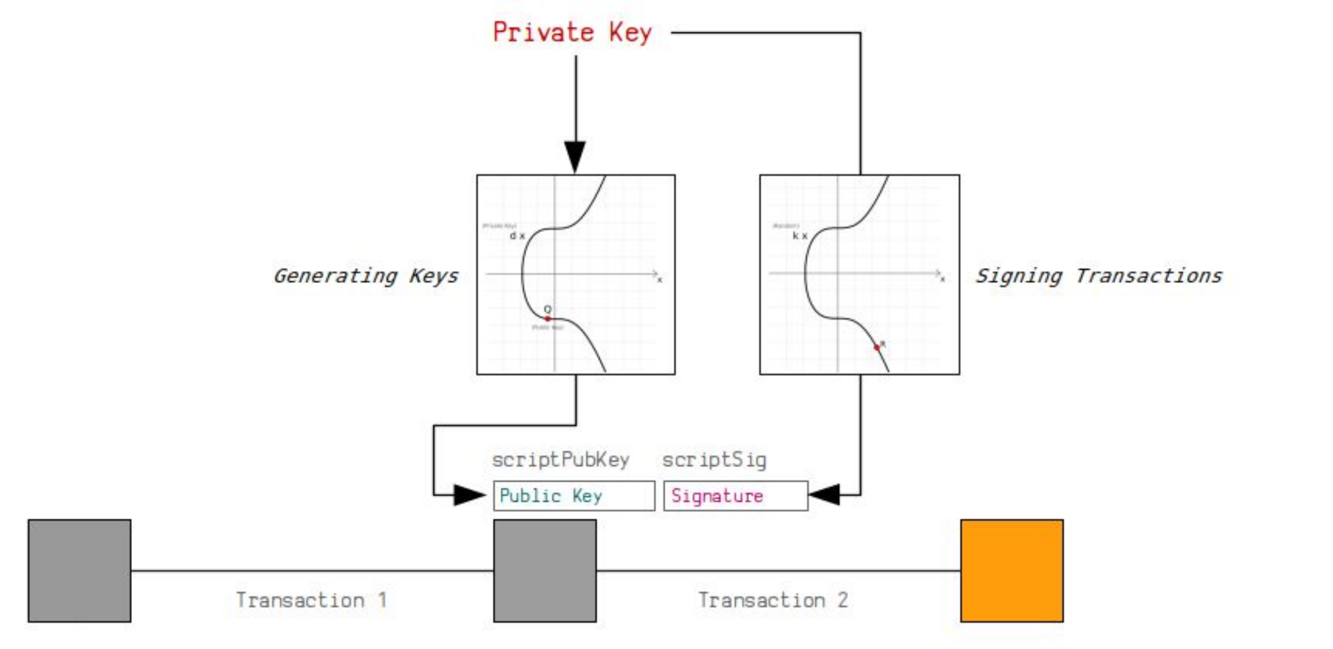
Back to Cryptography

RSA Key Pair

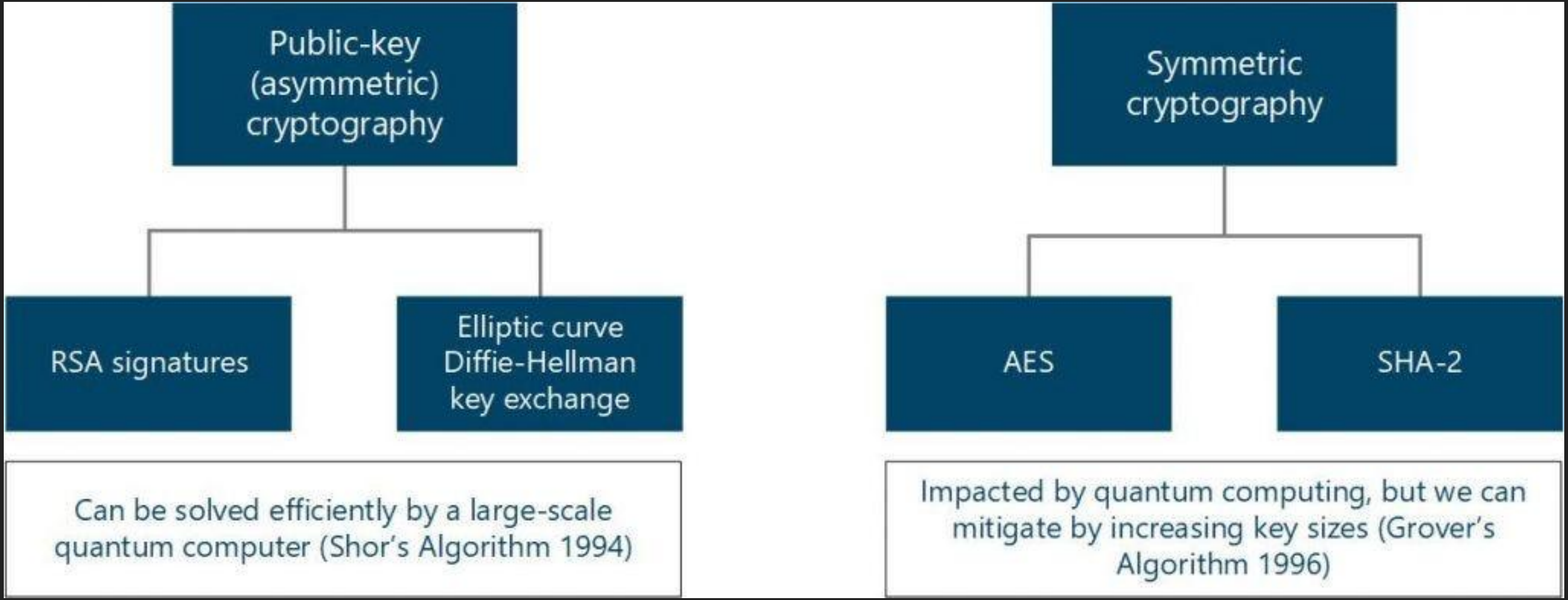
hackersvilla.xyz



ECDSA


Private Key
Generating Keys
(Private Key)
d x
x
Q
(Public Key)
(Random)
k x
x
R
Signing Transactions
scriptPubKey
scriptSig
Public Key
Signature
Transaction 1
Transaction 2

Impact on Encryption



Public-key (asymmetric) cryptography

RSA signatures

Elliptic curve Diffie-Hellman key exchange

Can be solved efficiently by a large-scale quantum computer (Shor's Algorithm 1994)

Symmetric cryptography

AES

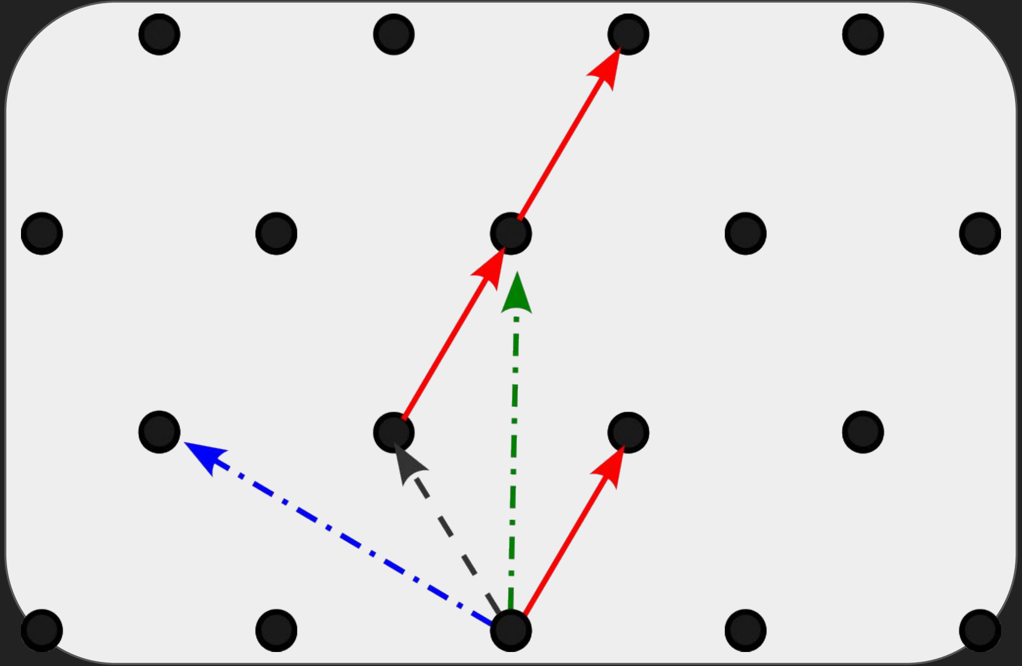
SHA-2

Impacted by quantum computing, but we can mitigate by increasing key sizes (Grover's Algorithm 1996)

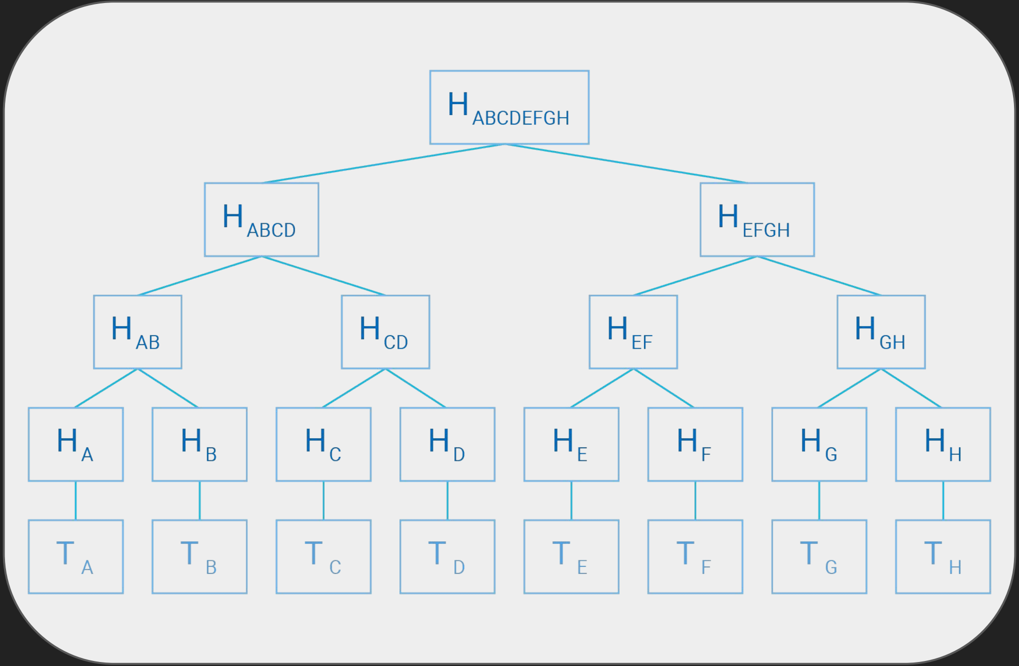
Post-Quantum Cryptography

hackersvilla.xyz

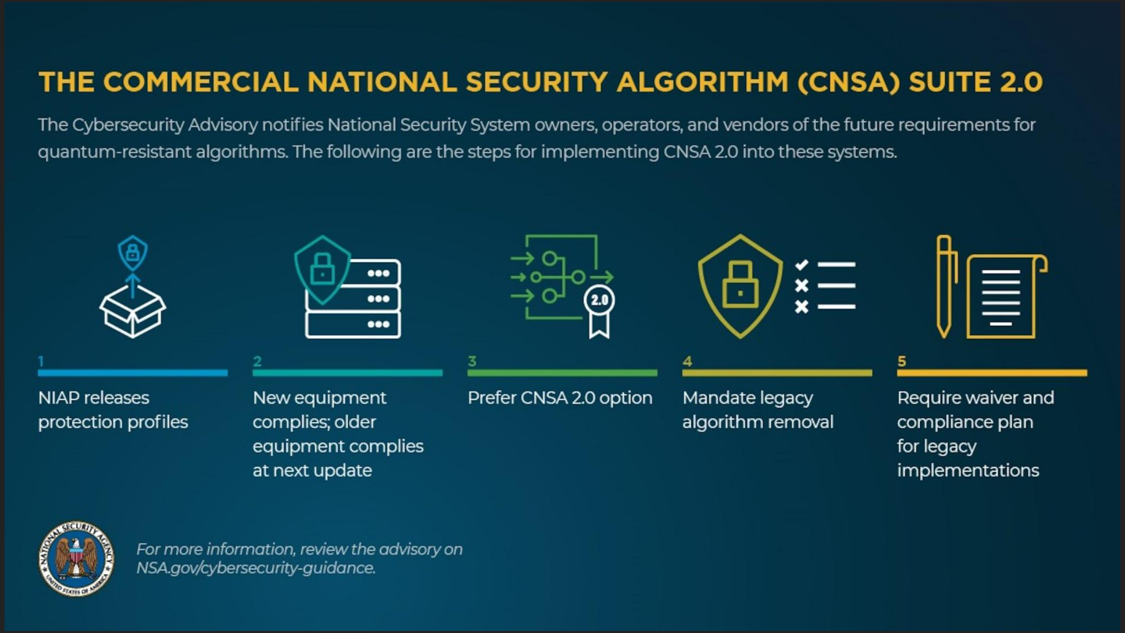
Lattice-Based Cryptography



Hash-Based Cryptography



Diverse Quantum-Resistant Algorithms



THE COMMERCIAL NATIONAL SECURITY ALGORITHM (CNSA) SUITE 2.0

The Cybersecurity Advisory notifies National Security System owners, operators, and vendors of the future requirements for quantum-resistant algorithms. The following are the steps for implementing CNSA 2.0 into these systems.

1 NIAP releases protection profiles

2 New equipment complies; older equipment complies at next update

3 Prefer CNSA 2.0 option

4 Mandate legacy algorithm removal

5 Require waiver and compliance plan for legacy implementations

For more information, review the advisory on NSA.gov/cybersecurity-guidance.

Implementation Challenges

Transitioning to quantum-resistant algorithms may come with increased computational requirements
Ongoing efforts to optimize and streamline the implementation of quantum-resistant algorithms to minimize computational overhead.

The need for a transitional period where both classical and quantum-resistant algorithms may coexist
Establishing global standards and protocols to ensure smooth interoperability during the transition.

Public awareness and education regarding the shift to quantum-resistant algorithms
Collaboration between industry, academia, and policymakers to facilitate widespread adoption.

What if we overcome the Challenges

Detection of Leak:
It allows the detection of data leak or hacking because it can detect any such attempt

Predetermined Error Levels:
It also allows the process of setting the error level between the intercepted data.

Unbreakable Encryption:
The encryption is unbreakable and that’s mainly because of the way data is carried via the photon.
A photon cannot be perfectly copied and any attempt to measure it will disturb it.
This means that a person trying to intercept the data will leave a trace.

Thank you for your active engagement in the talk.

Now, I invite **any questions** or discussions you may have.