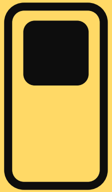
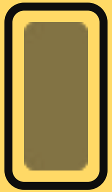
QUANTUM COMPUTERS & CYBERSECURITY

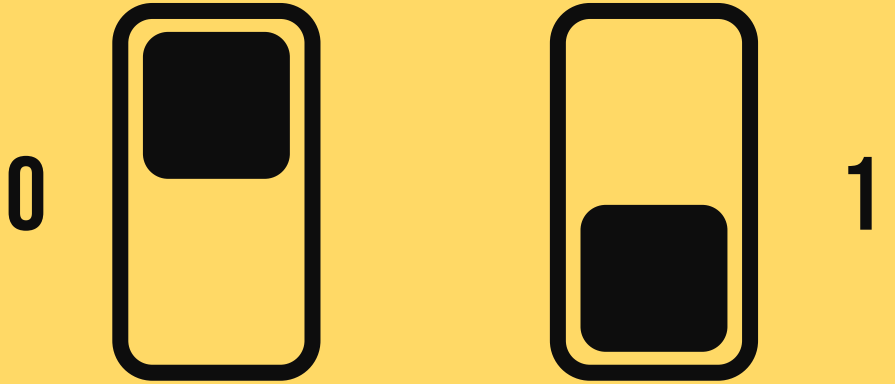
QUANTUM COMPUTERS



VS



CLASSICAL BITS



TWO DEFINITE STATES

LIMITATIONS

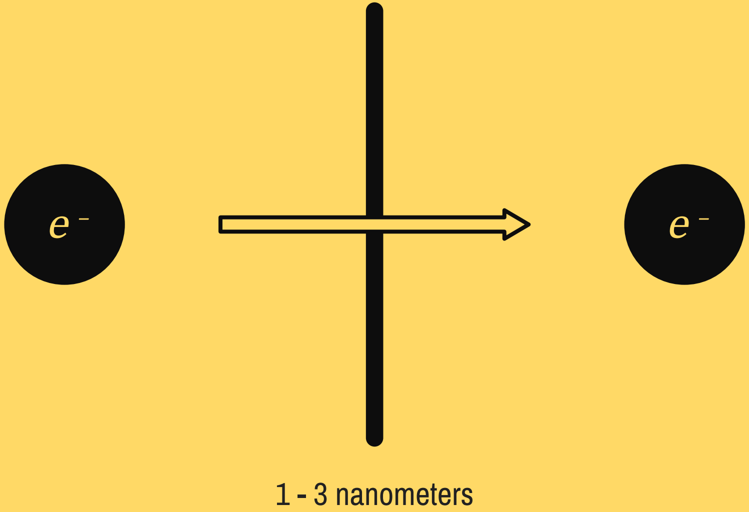
1 **Space**

Physical limit on bit size

2 **Time**

Large processing time for large datasets

QUANTUM TUNNELING

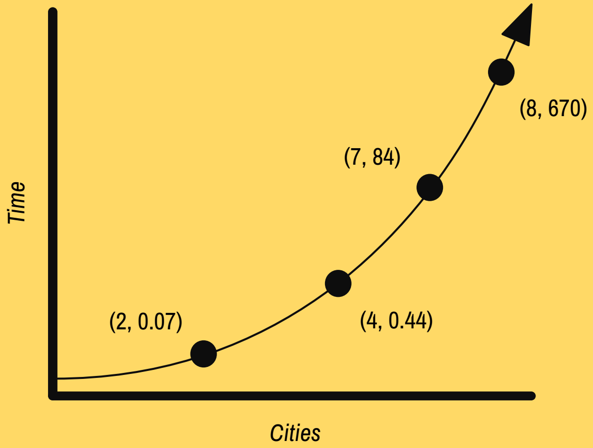


QUANTUM TUNNELING

EXAMPLE

TRAVELLING SALESMAN

Exponential computation time



SCAN ME

GOING QUANTUM

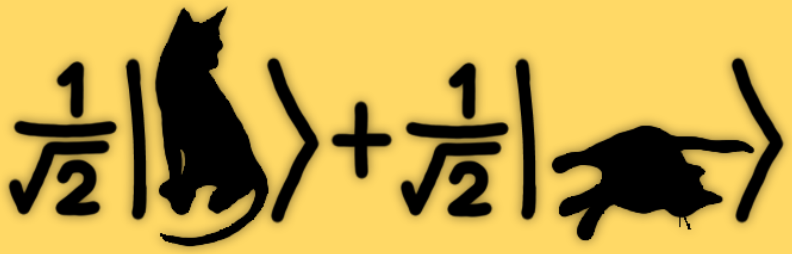
Utilizing fundamental properties of subatomic particles for computation

QUBIT NATURE

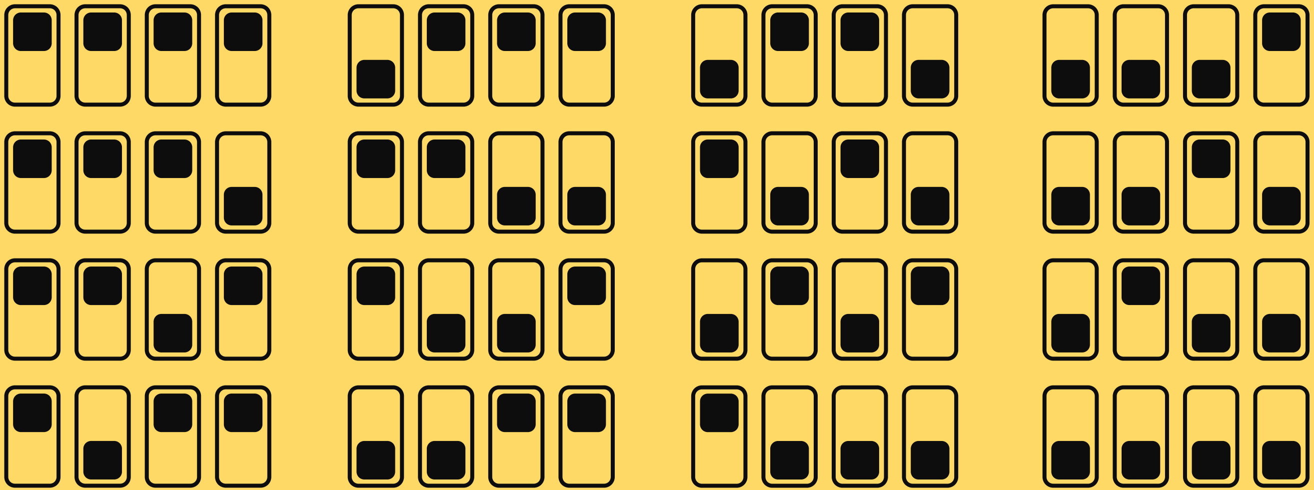
Ideal qubits remain in a state of
superposition

X%
Spin Up

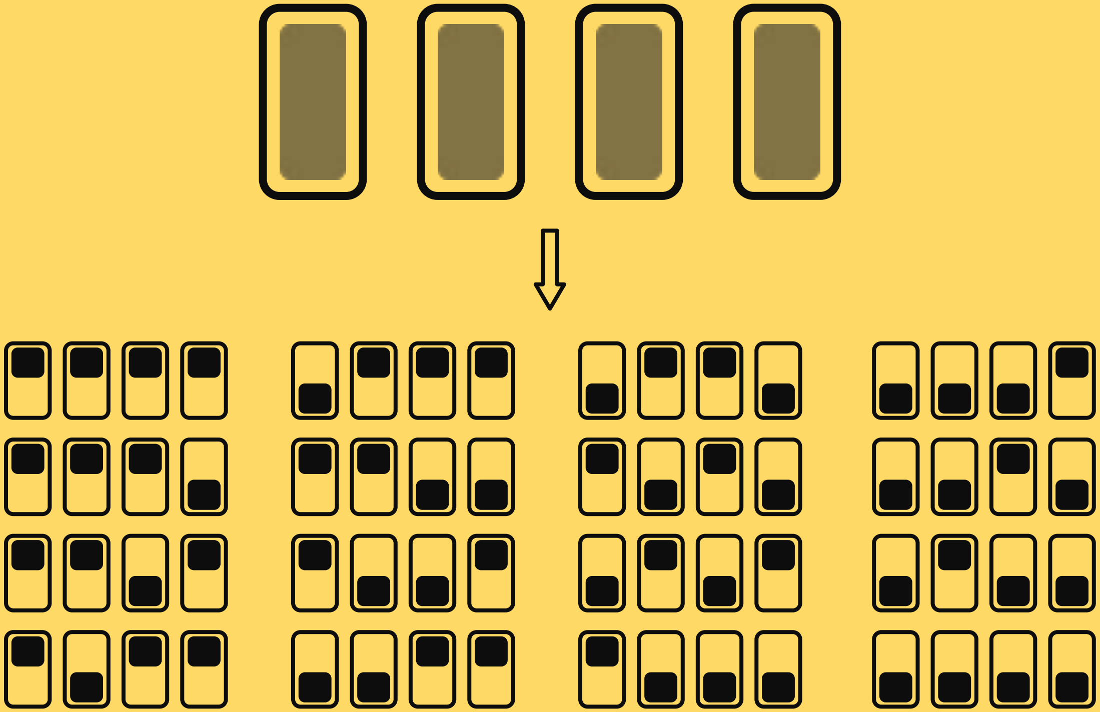
(1-X)%
Spin Down



SCHRODINGER'S CAT & SUPERPOSITION



64 bits, 16 combinations

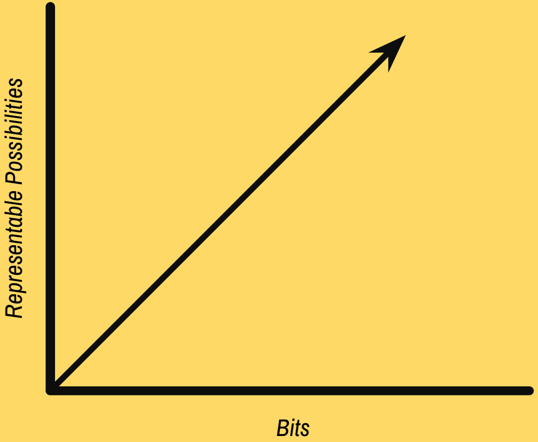


4 qubits, 16 combinations

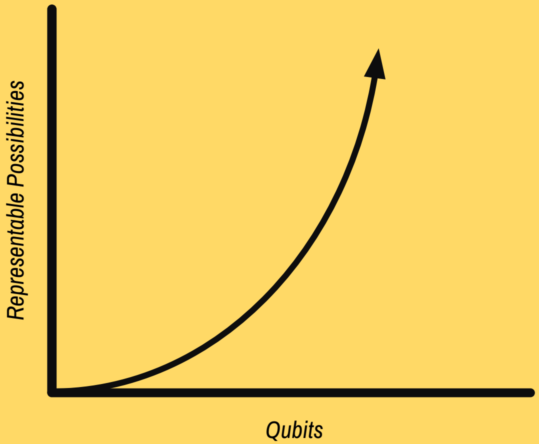
2^n *possibilities*

Where *n* represents the number of **qubits**

REPRESENTABLE POSSIBILITIES

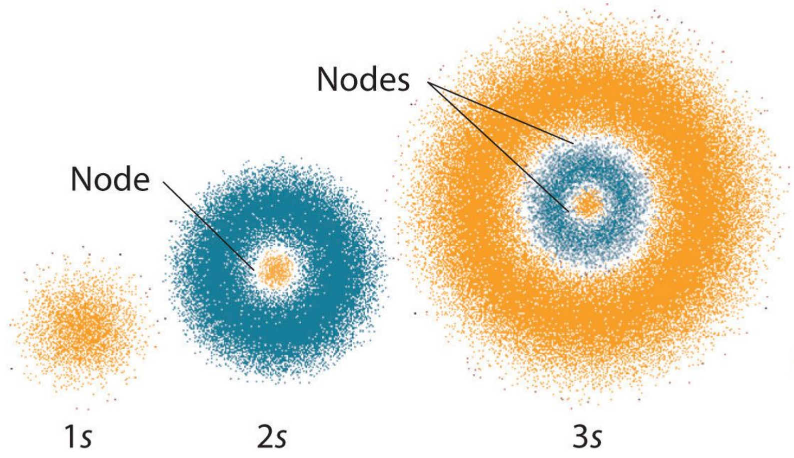


LINEAR GROWTH

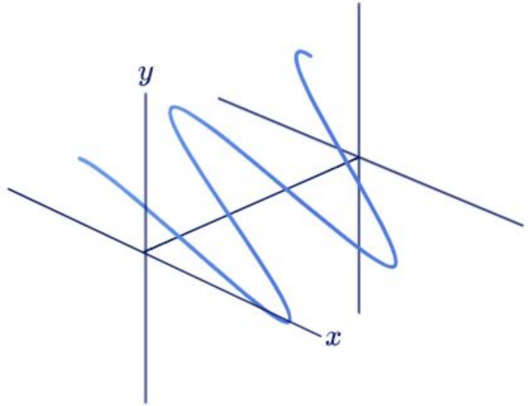


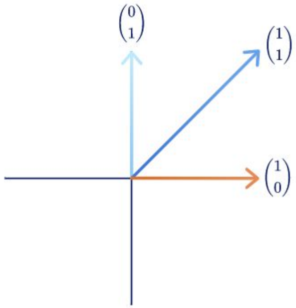
EXPONENTIAL GROWTH

POSITIONAL PROBABILITY

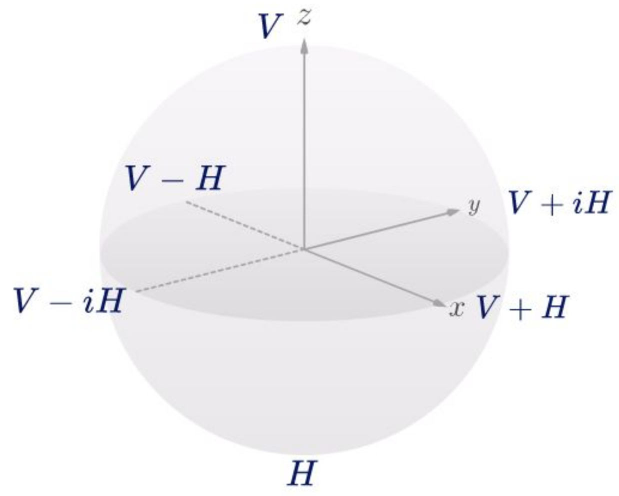


AMPLITUDES





BLOCH SPHERE

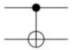
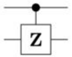
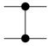
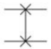
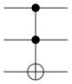


GATES

Transmitted wave (left), blocked wave (right)

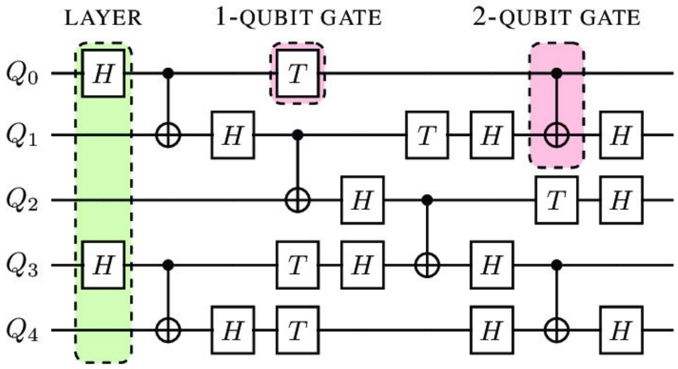
Blocked wave (left), transmitted wave (right)

GATES IN CIRCUITS

Operator	Gate(s)		Matrix
Pauli-X (X)	$\boxed{X}$	$\oplus$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	$\boxed{Y}$		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	$\boxed{Z}$		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)	$\boxed{H}$		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)	$\boxed{S}$		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)	$\boxed{T}$		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)			$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

QUANTUM CIRCUITS

SCAN ME



SO WHAT?

How are quantum circuits ***useful***?


INTERNET

SENDING & RECEIVING DATA

Encryption

Data is encrypted with a ***public key***

Sending

Packets are ***routed*** through the internet

Decryption

Received packets are decrypted with a ***private key***

RSA ENCRYPTION

RIVEST-SHAMIR-ADLEMAN

Easy to encode, hard to decode, and popular

Encryption key (public) = ($\boldsymbol{i}$, $\boldsymbol{M}$)

→ **Ciphertext** = S [(B (`string`)$^{\boldsymbol{i}}$) % $\boldsymbol{M}$]

Decryption key (private) = ($\boldsymbol{n}$, $\boldsymbol{M}$)

→ **Original Text** = S [(B (`ciphertext`)$^{\boldsymbol{n}}$) % $\boldsymbol{M}$]

ENCRYPTION & DECRYPTION

DECRYPTION KEY GENERATION

Secret primes = ($\boldsymbol{x}$, $\boldsymbol{y}$)

→ **Product** = $\boldsymbol{xy}$
→ **Number of Coprimes** = ($\boldsymbol{x}$ - 1)($\boldsymbol{x}$ - 1) = $\boldsymbol{C}$

$\boldsymbol{i}$ (encryption) ⇒ { 1 < $\boldsymbol{i}$ < $\boldsymbol{C}$, coprime with $\boldsymbol{C}$ and $\boldsymbol{xy}$ }

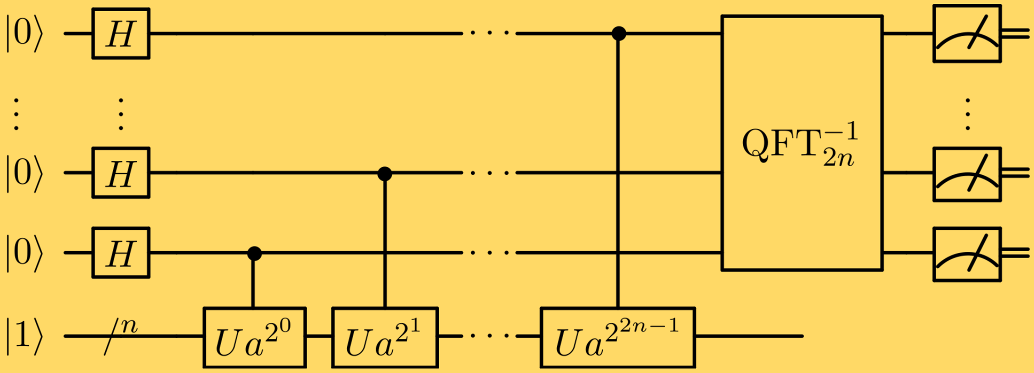
→ **Encryption Key** = ($\boldsymbol{i}$, $\boldsymbol{M}$)

$\boldsymbol{n}$ (decryption) ⇒ $\boldsymbol{ni}$ % $\boldsymbol{C}$ = 1

→ **Decryption Key** = ($\boldsymbol{n}$, $\boldsymbol{M}$)

$$G' = G^{P/2} \pm 1$$

Shor's Algorithm



BUT...

SHOULD WE?

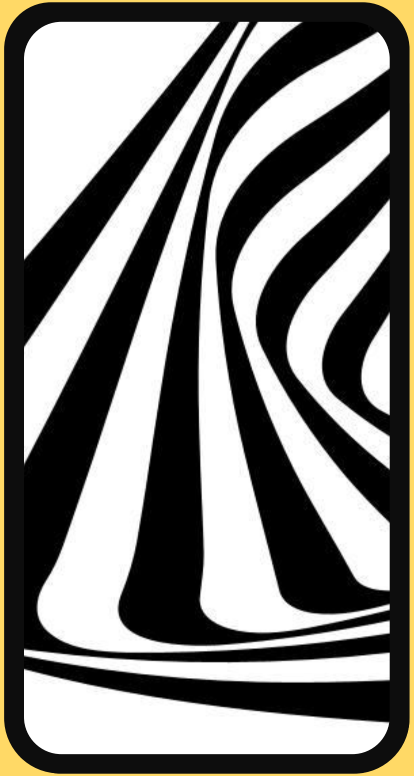
IMPACTS

How does QC + CS affect the world?

Public Scare

Hacking

World Power



USELESS FOR THE *AVERAGE CONSUMER*

OPERATING TEMP:

15 MILLIKELVIN

OVER

90%

QUANTUM RESISTANT ALGORITHMS

1

CRYSTALS-Kyber

For general encryption, fast and simple

2

CRYSTALS-Dilithium

For digital signatures, based on structured lattices

3

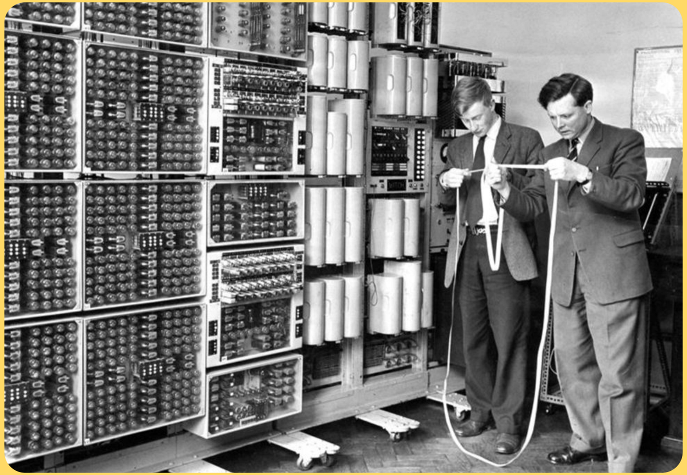
FALCON

For digital signatures, based on structured lattices

4

SPHINCS+

For digital signatures, based on hash functions



FINAL THOUGHTS:

WHAT SHOULD WE DO?