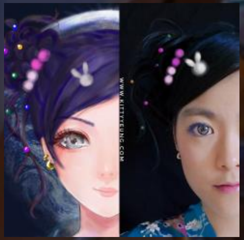
Introduction to Quantum Computing



Kitty Yeung, Ph.D. in Applied Physics

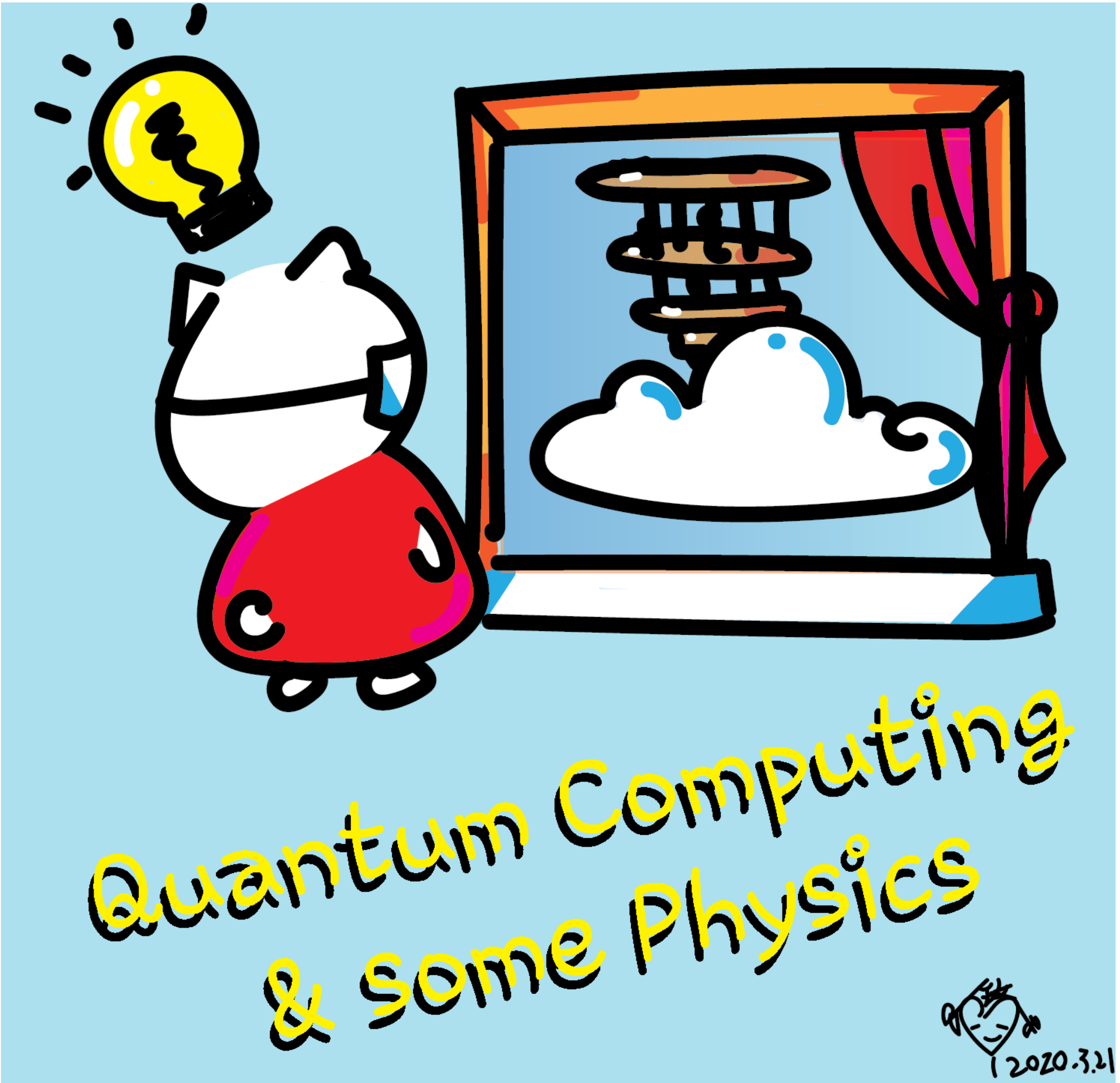
Creative Technologist + Sr. PM
Microsoft

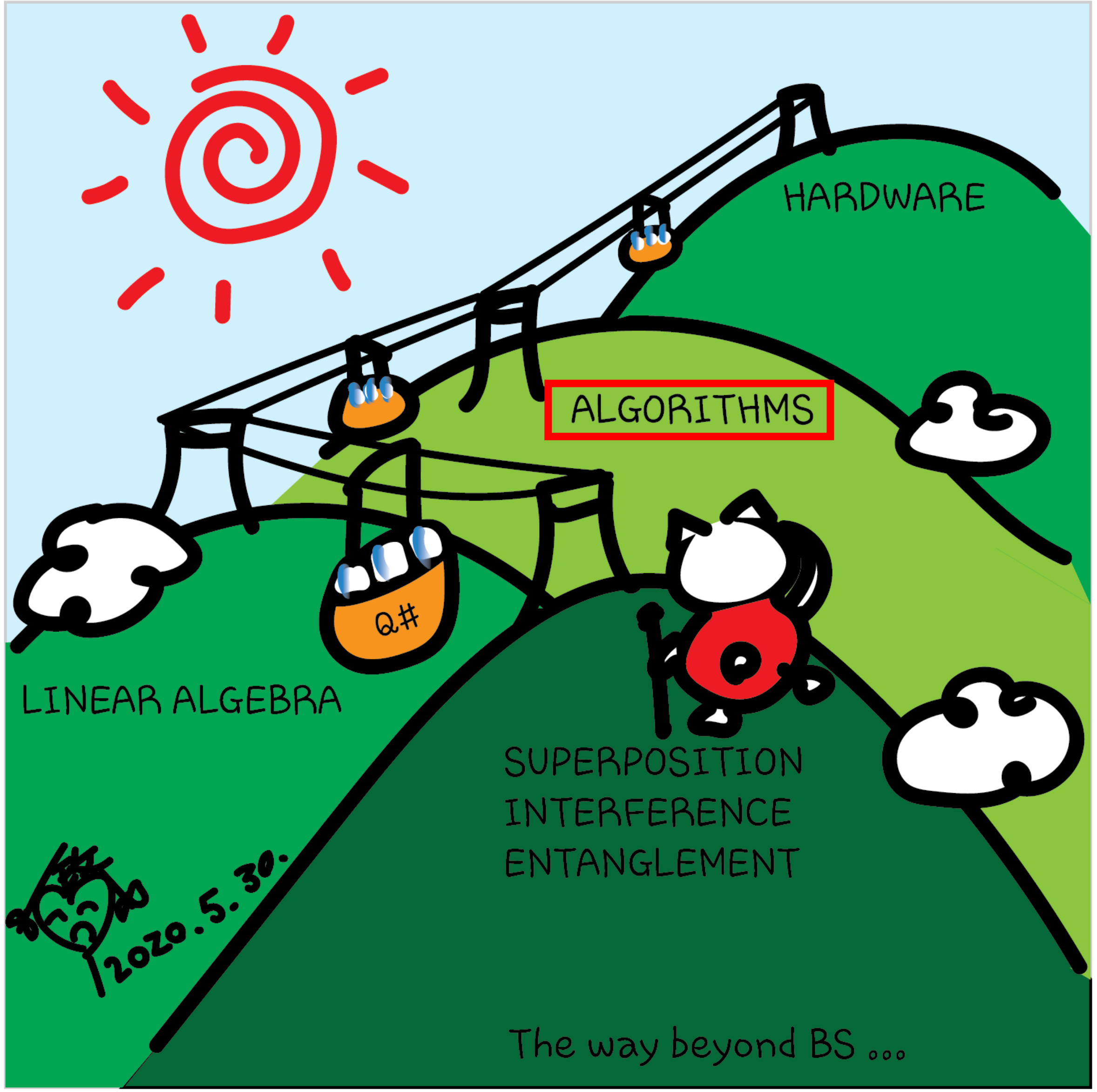
www.artbyphysicistkittyyeung.com
@KittyArtPhysics
@artbyphysicistkittyyeung

August 9, 2020
Hackaday, session 17
Other communities, session 9

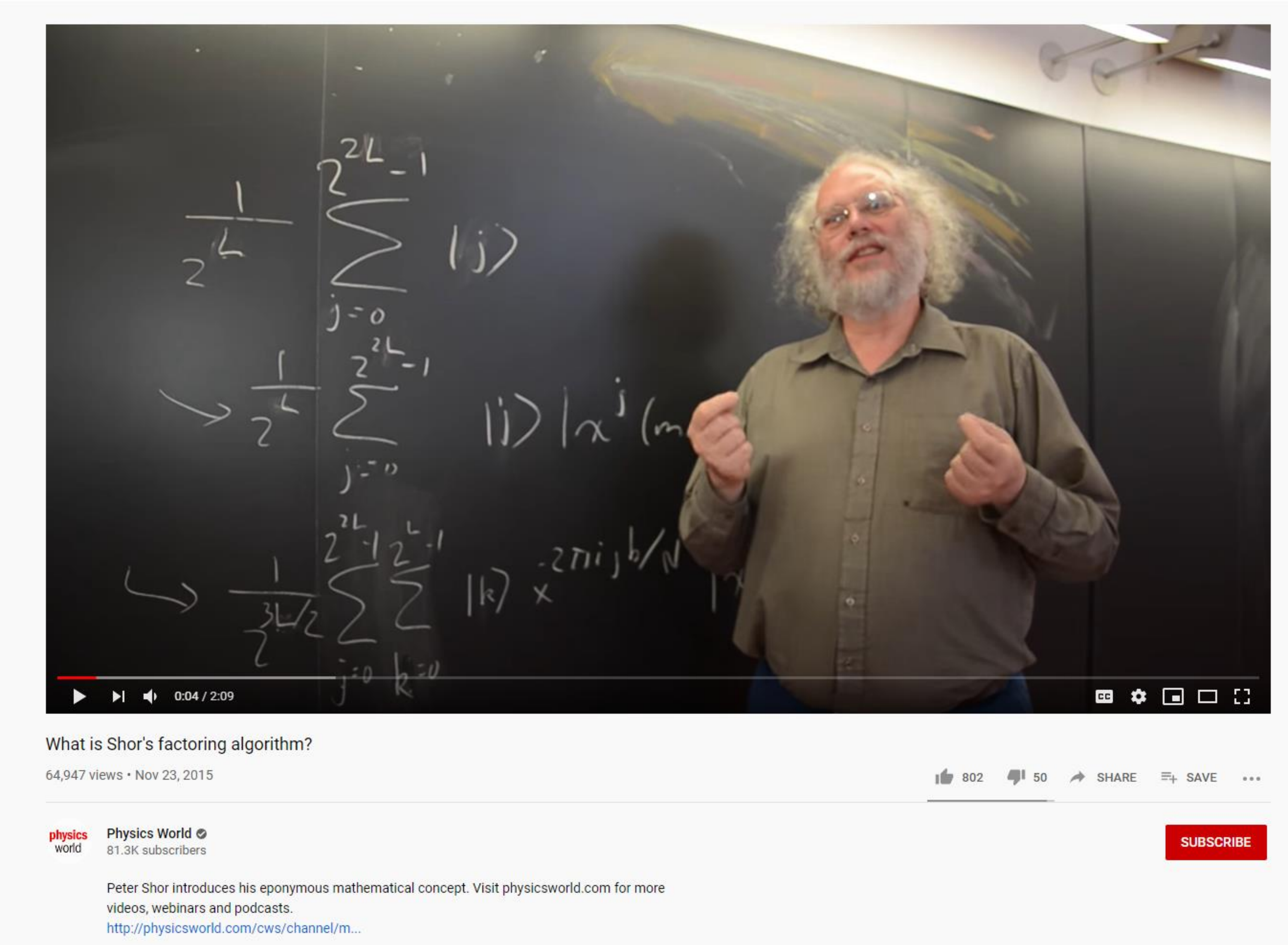
Class structure

- Comics on Hackaday – Quantum Computing through Comics every Sun
- 30 mins – 1 hour every Sun, one concept (theory, hardware, programming), Q&A
- Contribute to Q# documentation http://docs.microsoft.com/quantum
- Coding through Quantum Katas https://github.com/Microsoft/QuantumKatas/
- Discuss in Hackaday project comments throughout the week
- Take notes





The way beyond BS ...



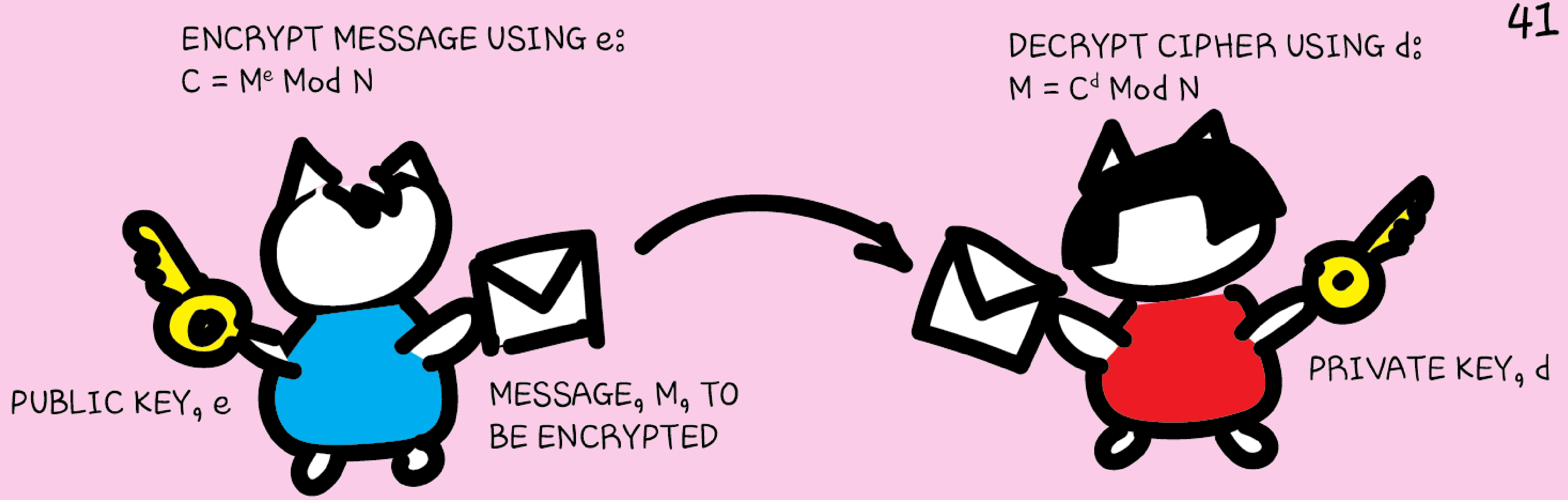
What is Shor's factoring algorithm?

64,947 views • Nov 23, 2015

Physics World
81.3K subscribers

Peter Shor introduces his eponymous mathematical concept. Visit physicsworld.com for more videos, webinars and podcasts.
http://physicsworld.com/cws/channel/m...

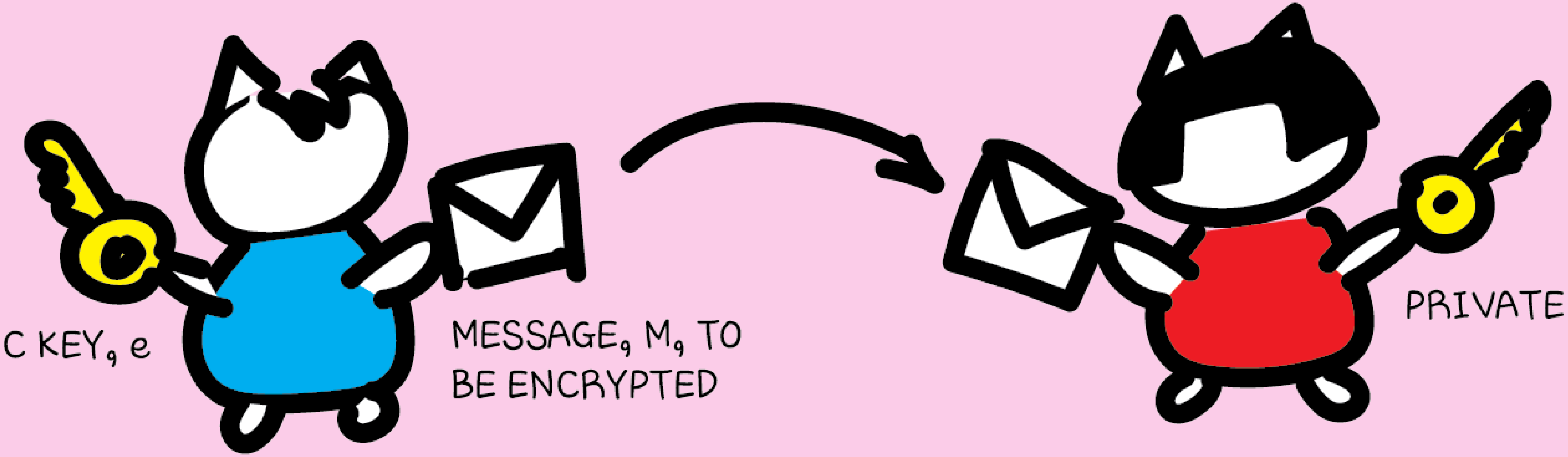
invented in 1994 by the American mathematician Peter Shor



THE RSA ENCRYPTION SCHEME

ENCRYPT MESSAGE USING e:
$C = M^e \text{ Mod } N$

DECRYPT CIPHER USING d:
$M = C^d \text{ Mod } N$



THE RSA ENCRYPTION SCHEME

$M^{ed} \text{ Mod } N = M$
$N=p*q$
$r = (p-1)(q-1)$
$e*d \text{ Mod } r = 1$

PUBLIC: N, e
PRIVATE: p, q, d, r

N is really large – it is infeasible to factorize it classically to get p and q, thus, d and r.

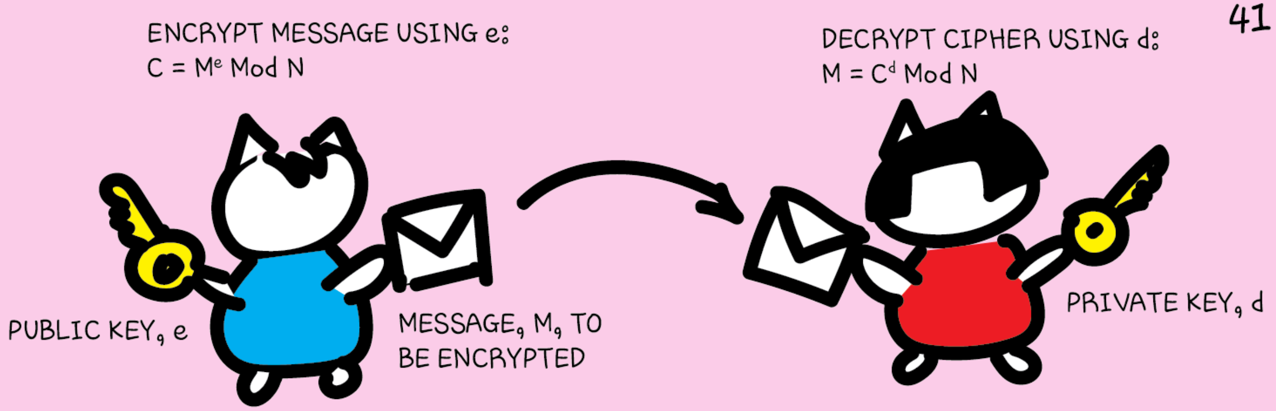
Example

- p = 101 and q = 113
- N = $p * q$ = 101 $*$ 113 = 11413
- r = (p – 1)(q – 1) = (101 – 1)(113 – 1) = 11200
- Find two numbers $\boldsymbol{e}$ and $\boldsymbol{d}$ that are relatively prime to $\boldsymbol{N}$ and for which $\boldsymbol{e} * \boldsymbol{d}$ = $\mathbf{1}$ mod r
- Say $\boldsymbol{e}$ = 13
- Then d = 9477 so that $e * d$ $m$od r = 1
- $e * d$ = 123201

Example

- $m$sg = 123
- Encrypted message = cipher = (m)^e $m$od N = (123)^13 $m$od 11413 = 5790

- Decrypted message = $m$sg = (cipher)^d $m$od N = 5790^9477 $m$od 11413 = 123



THE RSA ENCRYPTION SCHEME

M^{ed} Mod N = M

N=p*q

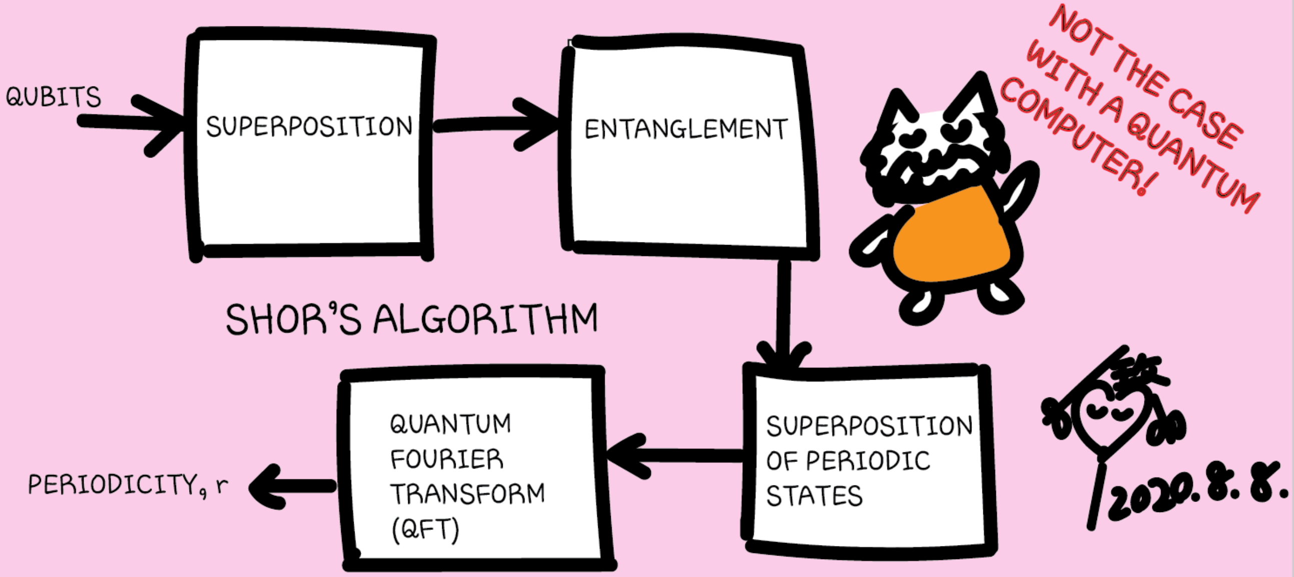
r = (p−1)(q−1)

e*d Mod r = 1

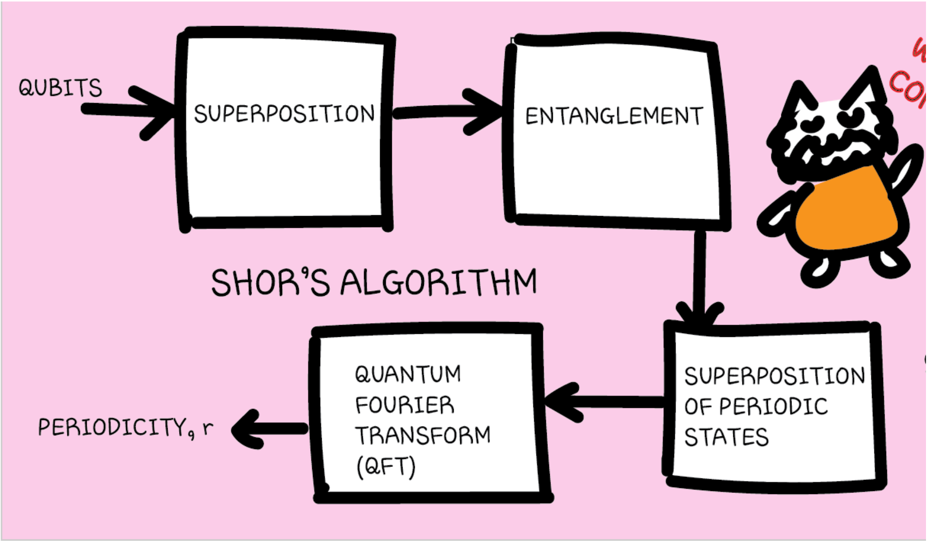
PUBLIC: N, e

PRIVATE: p, q, d, r

N is really large – it is infeasible to factorize it classically to get p and q, thus, d and r.

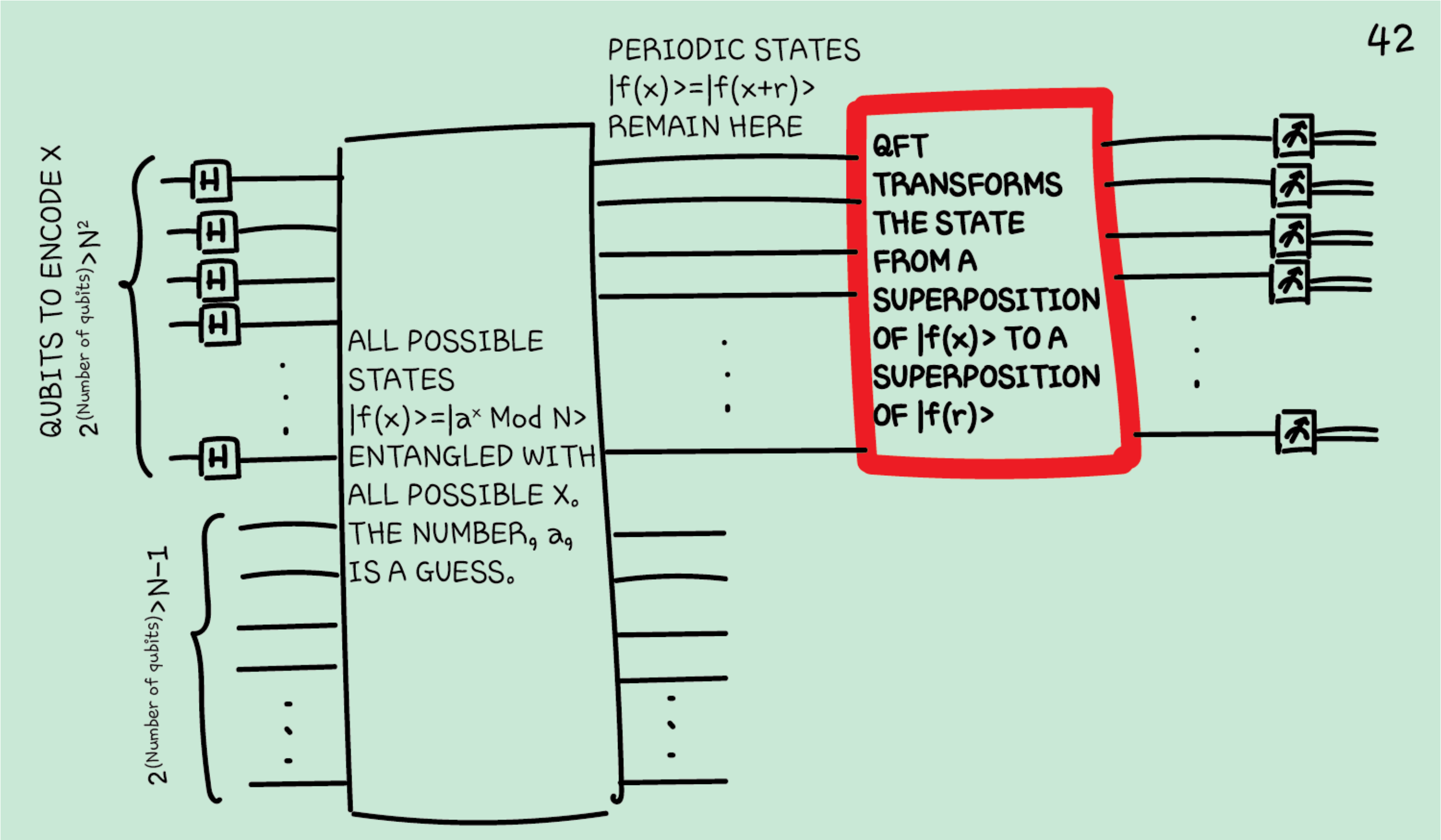

NOT THE CASE WITH A QUANTUM COMPUTER!
QUBITS
SUPERPOSITION
ENTANGLEMENT
SUPERPOSITION OF PERIODIC STATES
QUANTUM FOURIER TRANSFORM (QFT)
PERIODICITY, r
2020.8.8.

SHOR'S ALGORITHM



SHOR'S ALGORITHM

QUBITS
SUPERPOSITION
ENTANGLEMENT
SUPERPOSITION OF PERIODIC STATES
QUANTUM FOURIER TRANSFORM (QFT)
PERIODICITY, r
W
CO

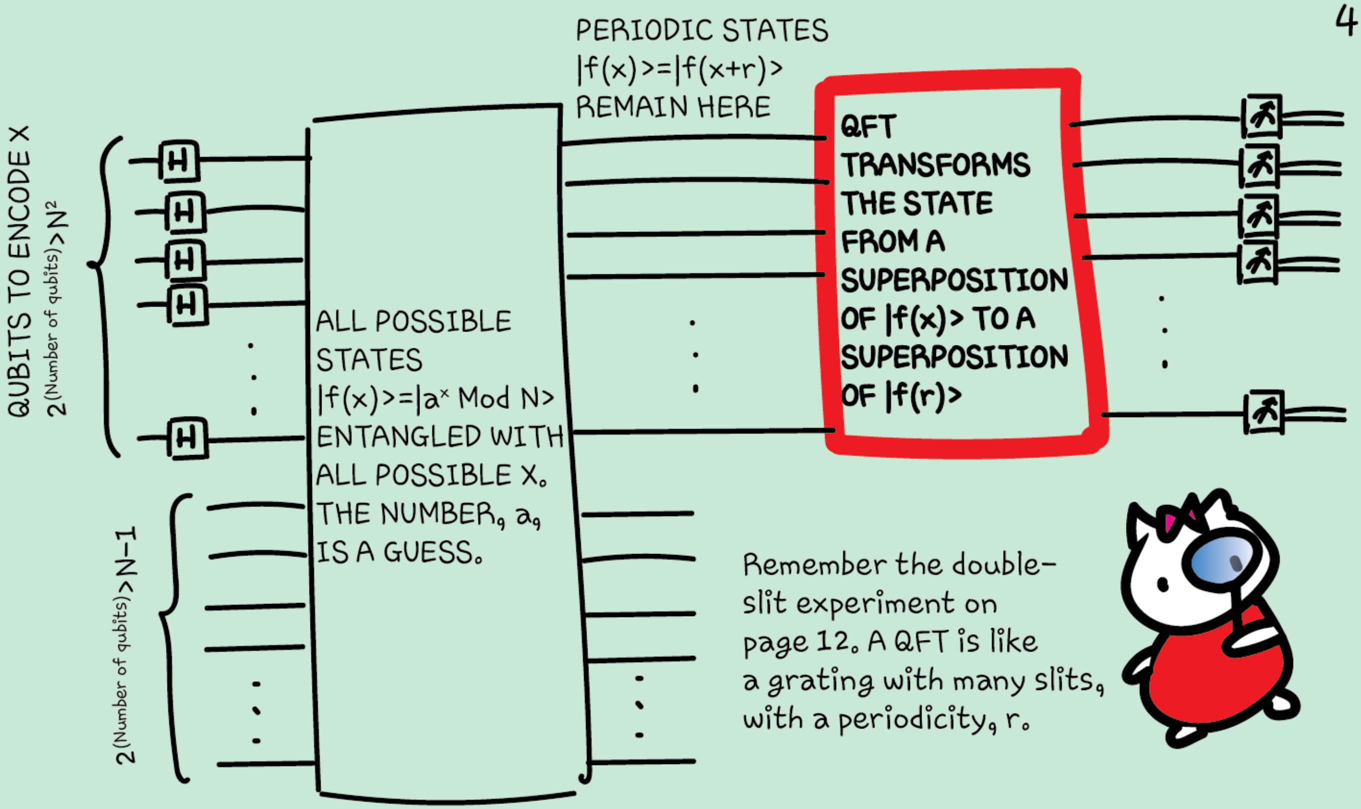


QUBITS TO ENCODE X
$2^{(\text{Number of qubits})} > N^2$
H
H
H
H
H
$2^{(\text{Number of qubits})} > N-1$

PERIODIC STATES $|f(x)\rangle = |f(x+r)\rangle$ REMAIN HERE

ALL POSSIBLE STATES $|f(x)\rangle = |a^x \text{ Mod } N\rangle$ ENTANGLED WITH ALL POSSIBLE X. THE NUMBER, a, IS A GUESS.

QFT TRANSFORMS THE STATE FROM A SUPERPOSITION OF $|f(x)\rangle$ TO A SUPERPOSITION OF $|f(r)\rangle$


QUBITS TO ENCODE X
$2^{(\text{Number of qubits})} > N^2$
H
H
H
H
H
$2^{(\text{Number of qubits})} > N-1$

PERIODIC STATES $|f(x)\rangle = |f(x+r)\rangle$ REMAIN HERE

ALL POSSIBLE STATES $|f(x)\rangle = |a^x \text{ Mod } N\rangle$ ENTANGLED WITH ALL POSSIBLE X. THE NUMBER, a, IS A GUESS.

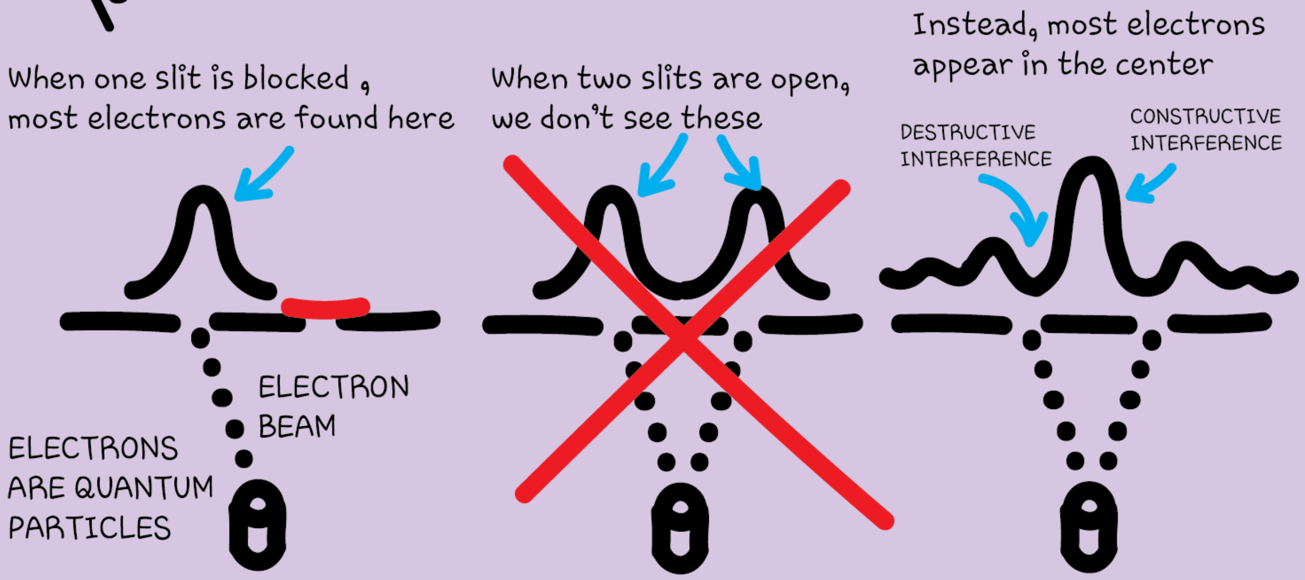
QFT TRANSFORMS THE STATE FROM A SUPERPOSITION OF $|f(x)\rangle$ TO A SUPERPOSITION OF $|f(r)\rangle$

Remember the double-slit experiment on page 12. A QFT is like a grating with many slits, with a periodicity, r.

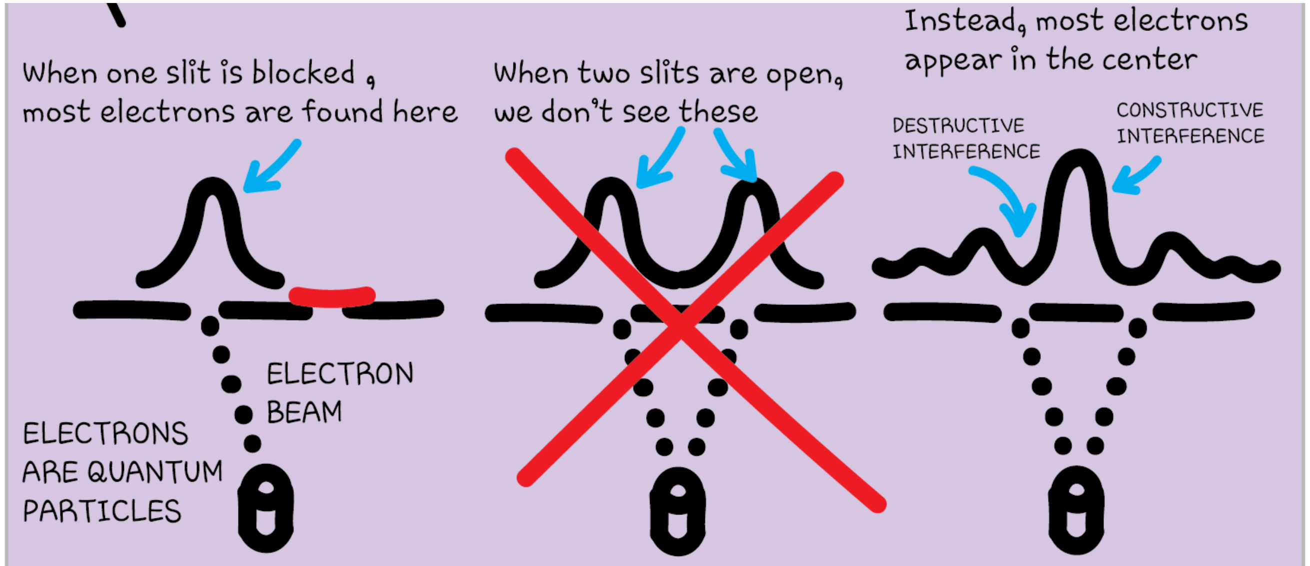
So, the things we observe (**measure**) are the results of interference. Possible results from constructive interference are more likely to be measured. The other possibilities cancel each other out through destructive interference.

2020.4.5.

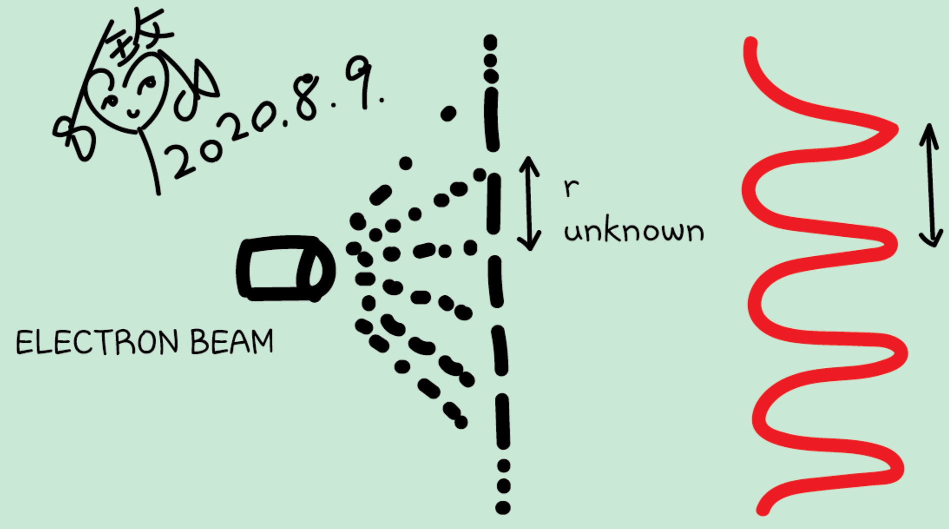
The famous double-slit experiment is a direct manifestation of quantum interference.


When one slit is blocked, most electrons are found here
ELECTRON BEAM
ELECTRONS ARE QUANTUM PARTICLES
When two slits are open, we don't see these
Instead, most electrons appear in the center
DESTRUCTIVE INTERFERENCE
CONSTRUCTIVE INTERFERENCE

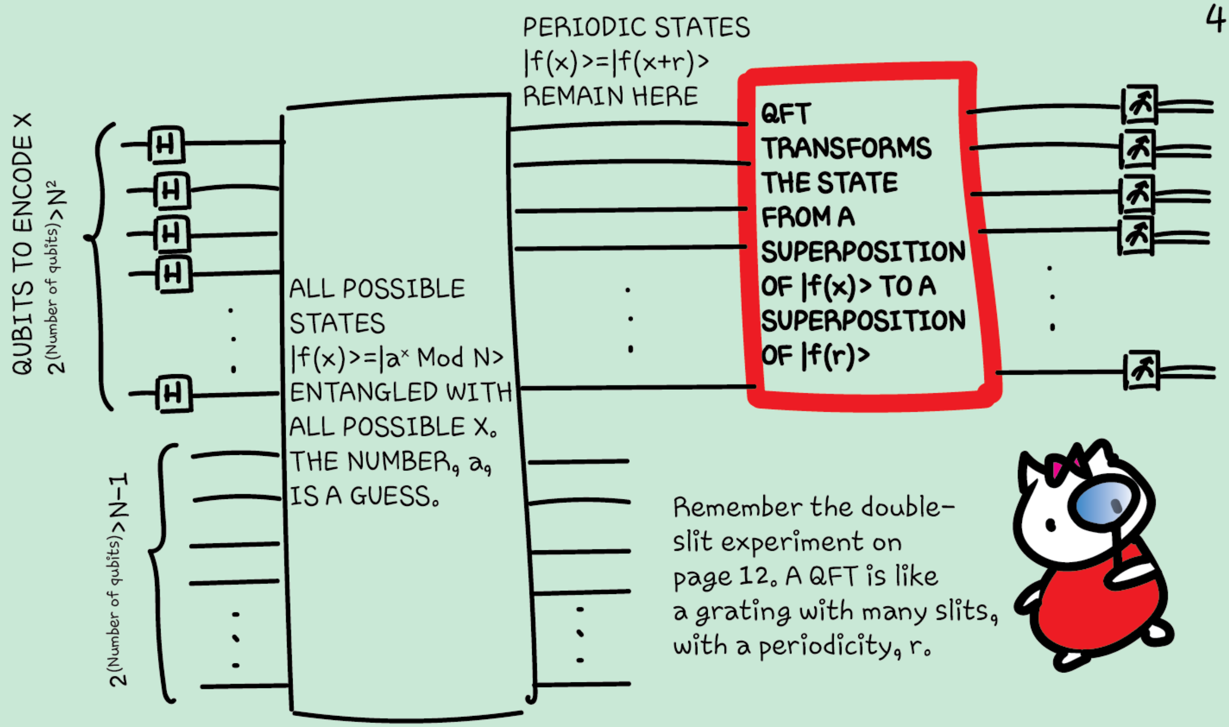
Interference is one of the "strange" behaviours of quantum systems enabled by superposition. What else?


When one slit is blocked, most electrons are found here
ELECTRON BEAM
ELECTRONS ARE QUANTUM PARTICLES
When two slits are open, we don't see these
Instead, most electrons appear in the center
DESTRUCTIVE INTERFERENCE
CONSTRUCTIVE INTERFERENCE

Interference is one of the "strange" behaviours of quantum systems enabled by superposition. What else?



The observed interference pattern is periodic with a pitch proportional to 1/r.



QUBITS TO ENCODE X

$2^{(\text{Number of qubits})} > N^2$

$2^{(\text{Number of qubits})} > N-1$

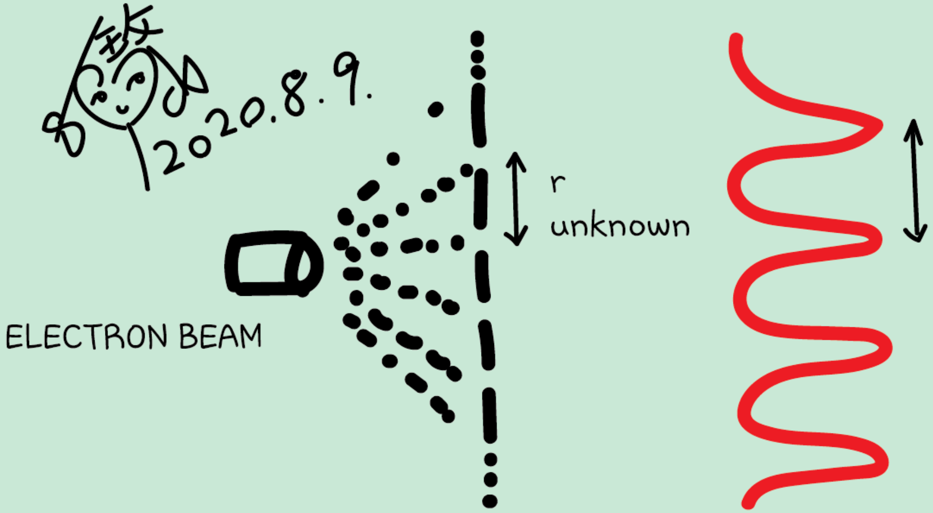
ALL POSSIBLE STATES $|f(x)\rangle = |a^x \text{ Mod } N\rangle$ ENTANGLED WITH ALL POSSIBLE X. THE NUMBER, a, IS A GUESS.

PERIODIC STATES $|f(x)\rangle = |f(x+r)\rangle$ REMAIN HERE

QFT TRANSFORMS THE STATE FROM A SUPERPOSITION OF $|f(x)\rangle$ TO A SUPERPOSITION OF $|f(r)\rangle$

Remember the double-slit experiment on page 12. A QFT is like a grating with many slits, with a periodicity, r.

2020.8.9.



The observed interference pattern is periodic with a pitch proportional to 1/r.

Shor’s Algorithm high-level videos

- How Quantum Computers Break Encryption | Shor's Algorithm Explained https://www.youtube.com/watch?v=lvTqbM5Dq4Q
- Hacking at Quantum Speed with Shor's Algorithm | Infinite Series https://www.youtube.com/watch?v=wUwZZaI5u0c&t=854s

Questions

- Post in chat or on Hackaday project https://hackaday.io/project/168554-quantum-computing-through-comics
- FAQ: Past Recordings on Hackaday project or my YouTube https://www.youtube.com/c/DrKittyYeung
- A quantum career Q&A session?