PHYS 142 LEC 19 — 30 May 2022

see LEC 18 notes on ENTANGLEMENT & TENSOR PRODUCTS
& SUPPLEMENTAL NOTES on RSA ENCRYPTION

QUANTUM COMPUTING

REFS: BERNHARDT, QUANTUM COMP...
NIELSEN & CHUANG
* MOORE & MERTENS
↳ The Nature of COMPUTATION

UNITARY OPS ARE LINEAR
↳ ACT on every component of a quantum state SIMULTANEOUSLY
⟶ test many solutions simultaneously

BUT YOU CAN TEST MANY SOLUTIONS W/ CLASSICAL COMPUTING
↳ monte carlo ALGORITHMS, SIMULATED ANNEALING

REAL POWER of QUANTUM: PARALLELISM + INTERFERENCE
↳ use constructive interference to make right answers more likely,
destructive interference to make wrong answers less likely.

HINT of SHOR'S ALGORITHM ← PERNHARDT.

SUPPOSE $N = p \times q$ (p, q PRIMES)

- PICK SOME a RDMN 1, N
- CHECK if a SHARES factors w/ N → if yes, you can find p or q
- ↙ NO
- CALCULATE $a \bmod N$, $a^2 \bmod N$, $a^3 \bmod (N)$
  ↳ this will eventually repeat w/ some PERIODICITY
  $a^r \bmod N = 1 \bmod N$
- CLAIM: GIVEN r, CAN USE CLASSICAL ALGO. to find p & q
- MAGIC: CALCULATE PERIOD w/ QUANTUM FOURIER TRANSFORM

RSA : Ref: youtube/wXB-V_KeiuB
Art of the Problem : public key cryptography (2012)

IDEA: PUBLIC KEY TO ENCRYPT
PRIVATE KEY TO DECRYPT
↑ hard to guess

MESSAGE ENCODED AS AN INTEGER, M

ENCODE: $M^E \bmod N = \tilde{M}$

PUBLIC KEY: (E, N)

N: some large #

$\tilde{M}$: ENCODED MESSAGE

EASY to DETERMINE $\tilde{M}$

BUT, GIVEN $\tilde{M}$, N, HARD to FIND M

↳ need to **trial & error**

WANT A WAY TO DECRYPT EASILY W/ PRIVATE KEY.

↳ eg $\tilde{M}^D \bmod N = M$

$(M^E)^D \bmod N = M$

$M^{ED} \bmod N = M$

ENCRYPTION DECRYPTION

WANT TO CONSTRUCT E & D WHERE IT IS HARD TO GUESS D.

how to construct D?

FACT: EULER TOTIENT FUNCTION, $\phi(n)$ IS THE # OF INTEGERS $\leq n$ W/ NO COMMON FACTORS W/ n

eg. $\phi(8) = 4 \leftarrow (1), 2, (3), 4, (5), 6, (7), 8$

$8 = 2^3$; 2 : 2^2 : 2×3 : 2^3

- when n is PRIME, $\phi(n) = n-1$
- MULTIPLICATION: $\phi(mn) = \phi(m)\,\phi(n)$
  - ↳ so if p, q are PRIME, $\boxed{\phi(pq) = (p-1)(q-1)}$
    ↳ EASY TO CALCULATE IF YOU KNOW p & q

EULER'S THM: $M^{\phi(N)} \bmod N = 1$

RAISE TO A POWER k:

$$M^{k\phi(N)} \bmod N = 1 \quad \leftarrow 1^k = 1$$

MULTIPLY BY M

$$\underbrace{M^{k\phi(N)+1} \bmod N}_{} = M$$

$$= M^{ED} \bmod N$$

E & $\phi(N)$ rel prime

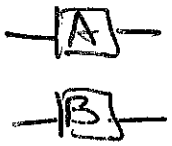
So: $ED = k\phi(N) + 1$

$$\boxed{D = \frac{k\phi(N)+1}{E}}$$ ← for integer k s.t. D is an integer.

RHS: EASY IF YOU KNOW $N = pq$
HARD to calc $\phi(N)$ otherwise
(LIKE TO FACTOR!)

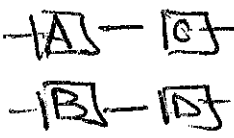
TENSORS IN CIRCUIT NOTATION

$|\psi\rangle$ —[U]— $|U\psi\rangle$ UNITARY OP U ACTING ON QUBIT $|\psi\rangle$



$= A \otimes B$, ACTS on tensor product STATE $|\psi_1\rangle \otimes |\psi_2\rangle$

eg $(A \otimes B)(C \otimes D) =$



$= (AC) \otimes (BD)$

nb: $\begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \otimes \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} = \begin{pmatrix} u_0 & v_0 \\ u_0 & v_1 \\ u_1 & v_0 \\ u_1 & v_1 \end{pmatrix}$

eg $|01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

$|01\rangle$ = $|0\rangle \otimes |1\rangle$

$$A \otimes B = \left(\begin{array}{c|c} A_{11}B & A_{12}B \\ \hline A_{21}B & A_{22}B \end{array}\right)$$

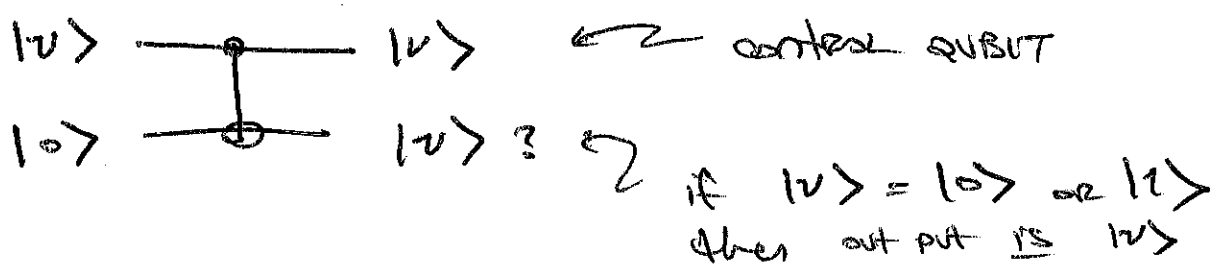
CONTROLLED NOT GATE (CNOT)

$|a,b\rangle \rightarrow |a, b \oplus a\rangle$

if $a=0 \Rightarrow b$

if $a=1 \Rightarrow$ SWAPS b $\uparrow \leftrightarrow \downarrow$

no cloning thm ← hard to copy a qubit



BUT IF $|\psi\rangle$ IS SUPERPOSITION ?

$$|\psi\rangle \otimes |\psi\rangle = v_0^2|00\rangle + v_0 v_1 (|01\rangle + |10\rangle) + v_1^2|11\rangle$$

$(v_0|0\rangle + v_1|1\rangle)$

BUT: $v_0|0\rangle \otimes |0\rangle + v_1|1\rangle \otimes |0\rangle$

no way any LINEAR OPERATOR CAN GIVE nonlinear terms in v_0 & v_1 !