QUANTUM CRYPTOGRAPHY (CS 598CTO)

Webpage: courses.grainger.illinois.edu/cs598cto/sp2022

OVERVIEW:

Part 1: * What computational powers do quantum mechanical systems bestow?

* What cryptosystems would break down if large scale quantum computers existed? Why?

* Which cryptosystems would remain secure? Why?

Part 2: * Harness quantum computers to build new cryptosystems that are unachievable by classical computers.

* quantum money

* quantum copy protection / software leasing

Messages exchanged are quantum, over "quantum" channels.

Admin details : dakshita@illinois.edu

* Please check your email.
* Please email me if you didn't get signed up for piazza.
* My OH : Tue 4-5 pm
* GRADING

10% : Participation in class

10% : Scribe Notes (1 per class)

30% : Assignments (3, all pre Spring break, 10 days per assignment)

50% : Videos and/or Projects

(already existing research) (new research)

Classical computing:

Turing Machine or
Circuit model

Extended C-T Hypothesis:

Any physically realizable computer can be simulated with poly overhead on a classical Turing Machine.

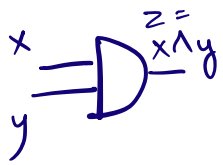
Quantum computers can factor products of large random primes.
May falsify ECTH!

Model of Quantum Computing:

Quantum Turing Machines or
Quantum circuits

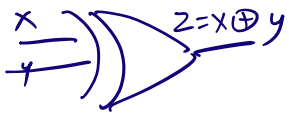
A measure of complexity: # gates in quantum circuit

AND



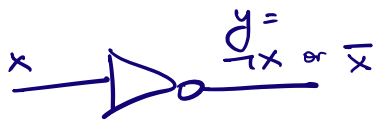
x	y	z
0	0	0
0	1	0
1	0	0
1	1	1

XOR



x	y	z
0	0	0
0	1	1
1	0	1
1	1	0

NOT

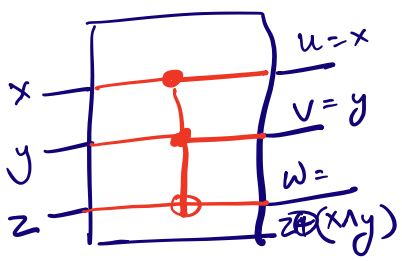


Given y, can you recover its input x?

$x = \neg y$ YES.

NOT is "reversible".

CCNOT (Toffoli)



Given u, v, w,

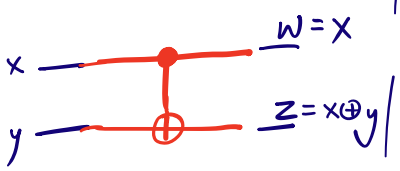
$x = u$

$y = v$

$z = w \oplus (u \wedge v)$.

CNOT

"Controlled" NOT



reversible?

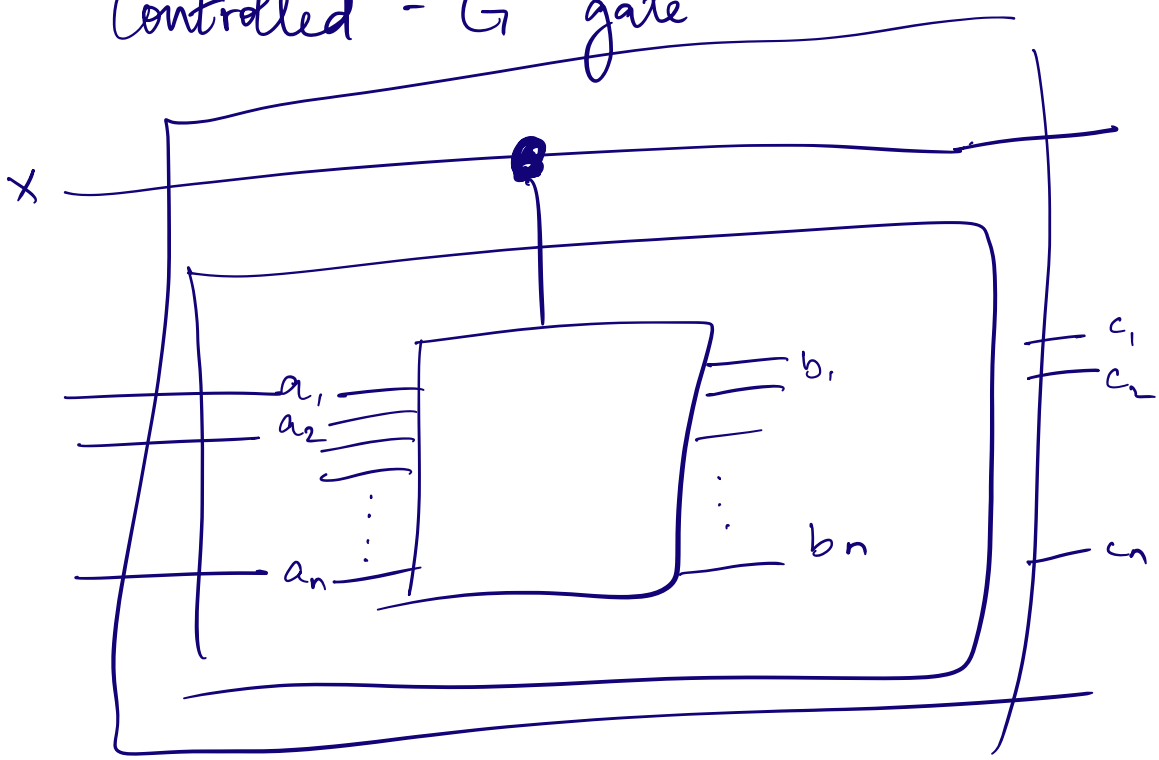
YES.

$$\begin{cases} x = w \\ y = z \oplus w \end{cases}$$

INPUT	OUTPUT
00	00
01	01
10	11
11	10

flip 2nd bit iff the 1st bit is 1

"Controlled" - G gate



if $x = 0$, then

$$c_1 c_2 \ldots c_n = a_1 a_2 \ldots a_n \quad \left(\begin{array}{c}\text{don't}\\ \text{apply}\\ G\end{array}\right)$$

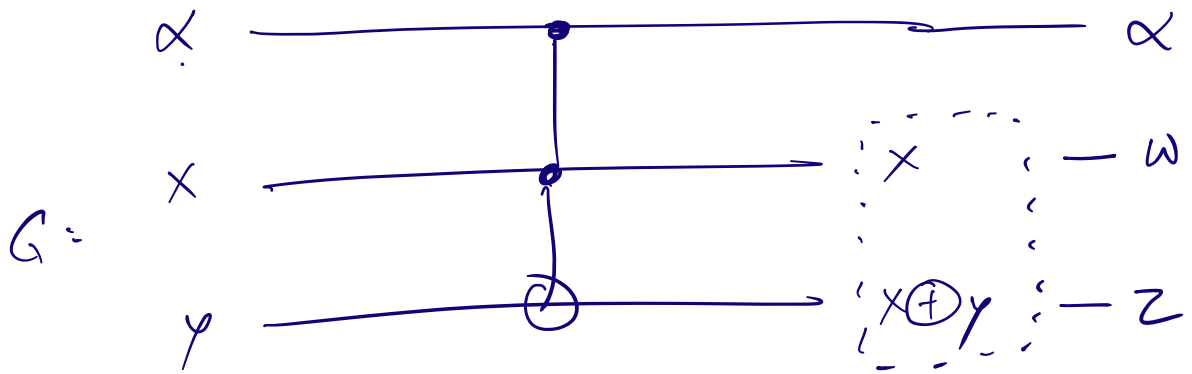
$x = 1$, then

$$= G(a_1 \ldots a_n)$$

$$c_1 c_2 \ldots c_n = b_1 b_2 \ldots b_n$$

$$\left(\begin{array}{c}\text{do}\\ G\end{array}\ \begin{array}{c}\text{apply}\\ \end{array}\right)$$

"Controlled" CNOT Gate



if $\alpha = 0$, $w = x$, $z = y$
(don't apply CNOT)

if $\alpha = 1$, $w = x$, $z = x \oplus y$
(do apply CNOT)

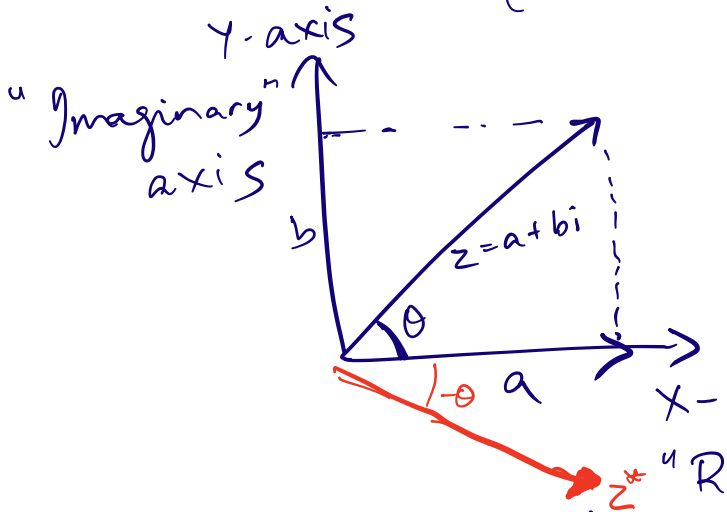
	INPUT	OUTPUT	
$\alpha = 0$	000	000	output = input when $\alpha = 0$
	001	001	
	010	010	
	011	011	
$\alpha = 1$	100	100	last 2 bits of output = CNOT(last 2 bits of input) when $\alpha = 1$
	101	101	
	110	111	
	111	110	

Complex Numbers

$a + bi \qquad a, b \in \mathbb{R}$

i imaginary unitary

$(i.e. \quad i^2 = -1)$



$$|z| = \sqrt{a^2 + b^2}$$

$$z = |z| \cos\theta + i|z| \sin\theta$$

$|z|$: radial coordinate; θ: angular coordinate

$$= |z| e^{i\theta} \qquad e^{i\theta} = (\cos\theta + i \sin\theta)$$

EULER'S FORMULA

Given $z_1 = |z_1| e^{i\theta_1}$, $z_2 = |z_2| e^{i\theta_2}$

$$z_1 z_2 = |z_1||z_2| e^{i(\theta_1 + \theta_2)}$$

$z^* = (a - bi)$ for $z = (a + bi)$

$$z z^* = (a+bi)(a-bi)$$

$$= a^2 - \cancel{ab} + \cancel{ab}i - b^2 \underbrace{i^2}_{=-1}$$

$$= a^2 + b^2$$

$$= |z|^2$$

Conjugate transpose of a matrix

$$U = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} a_1+b_1 i & a_2+b_2 i \\ a_3+b_3 i & a_4+b_4 i \end{bmatrix}$$

dagger

$$U^\dagger = \begin{bmatrix} \alpha^* & \gamma^* \\ \beta^* & \delta^* \end{bmatrix} = \begin{bmatrix} a_1-b_1 i & a_3-b_3 i \\ a_2-b_2 i & a_4-b_4 i \end{bmatrix}$$

(i.e. transpose the matrix and conjugate every term)

$$A = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \qquad A^* = \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix}$$

Two vectors A, B are <u>orthonormal</u> if the $A^* B = 0$.