Title: PSI 2018/2019 - Quantum Information Review - Lecture 8

Speakers: Daniel Gottesman

Collection: PSI 2018/2019 - Quantum Information Review (Gottesman)

Date: March 13, 2019 - 11:30 AM

URL: http://pirsa.org/19030045

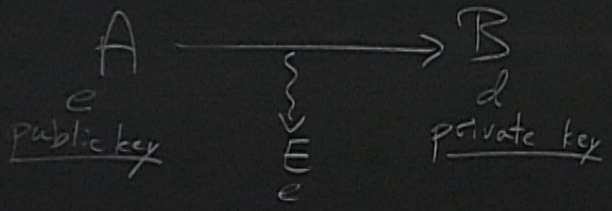
Factoring: Given N. Find $p, q > 1$ s.t. $N = pq$ if p & q exist.

$\Leftrightarrow$ Given N & M. Does N have a prime factor less than M?

Note: Multiplying p & q together is easy

Best known factoring algorithm takes $\sim \exp((\log N)^{1/3})$ steps.

Public key cryptosystem:



Symmetric encryption: A & B share same key.

Public key system: Public key e used to encrypt

Private key d used to decrypt.

RSA:

Key generation: Bob picks 2 large primes p & q.

Let $N = pq$. Bob also chooses some $e < N$ and finds d s.t. $x^{ed} = x \bmod N \ \forall x$.

Private key: d

Public key: (N, e)

Encryption: Alice has message x

Ciphertext $y = x^e \mod N$

Decryption: Bob receives y.

Calculates $y^d \mod N = x^{ed} \mod N$

$= x \mod N$ ✓

ge x

N

Thm (Euler's thm): $\forall x < N$, $x^{\varphi(N)} = 1 \bmod N$

$\varphi(N)$ is Euler's totient function, # of natural numbers $< N$ & relatively prime to N.

$N = pq$, p & q prime

$\varphi(N) = (p-1)(q-1)$

RSA:

Key generation: Bob picks 2 large primes p & q.

Let $N = pq$. Bob also chooses some $e < N$ and finds d s.t. $x^{ed} = x \bmod N \ \forall x$.

(e: relatively prime to $\varphi(N)$.)

Private key: d

Public key: (N, e)

Encryp

Ciph

Decrypt

Calcula

Thm (Euler's thm): $\forall x < N, \; x^{\varphi(N)} = 1 \bmod N$

$\varphi(N)$ is Euler's totient function, # of natural numbers $< N$ & relatively prime to N.

$N = pq$, p & q prime

$\varphi(N) = (p-1)(q-1)$

Using Euclid's algorithm, find d s.t.

$de = 1 \bmod \varphi(N) \Leftrightarrow de = 1 + c\varphi(N)$

Period Finding: Let $f: \mathbb{Z}_N \to \mathbb{Z}_N$ be a periodic function w/ period r that it does not otherwise repeat values. That is, $f(a) = f(b)$ iff $b = a + cr$

Find r

$de = 1 \bmod \varphi(N) \Leftrightarrow de = 1 + c\varphi(N)$

Claim: Factoring $N = pq$ reduces to finding the period of $f_x(a) = x^a \bmod N \ \forall x$.

Goal: Find x that has even order r (order is smallest r s.t. $x^r = 1 \bmod N$)

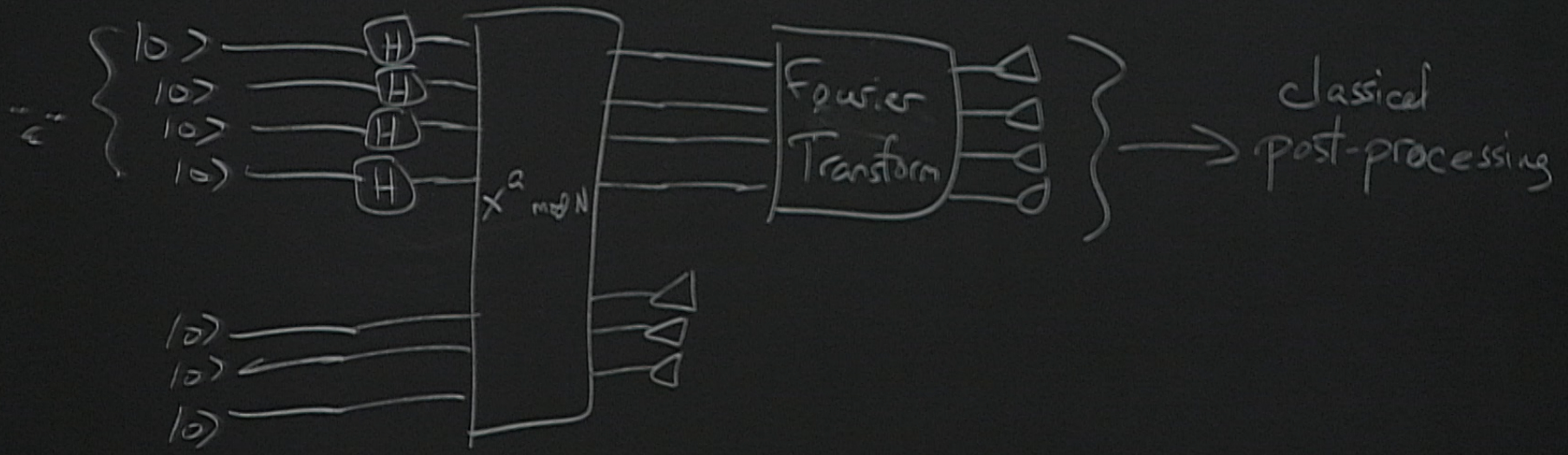
Let $y = x^{r/2}$. $y^2 = 1 \bmod N$. $\Rightarrow$ $y^2 - 1 = (y+1)(y-1) = kN = kpq$

$N \mid y+1$: $y = -1 \bmod N$. $\leftarrow$ With constant prob. (over x), this doesn't happen.

or $N \mid y-1$: No, r is the period

or $p \mid y+1$ & $q \mid y-1$: $GCD(N, y+1) = p$, $GCD(N, y-1) = q$ $\Rightarrow$ Find p & q using Euclid's algorithm

Shor's algorithm: x is given, find r s.t. $x^r = 1 \bmod N$.



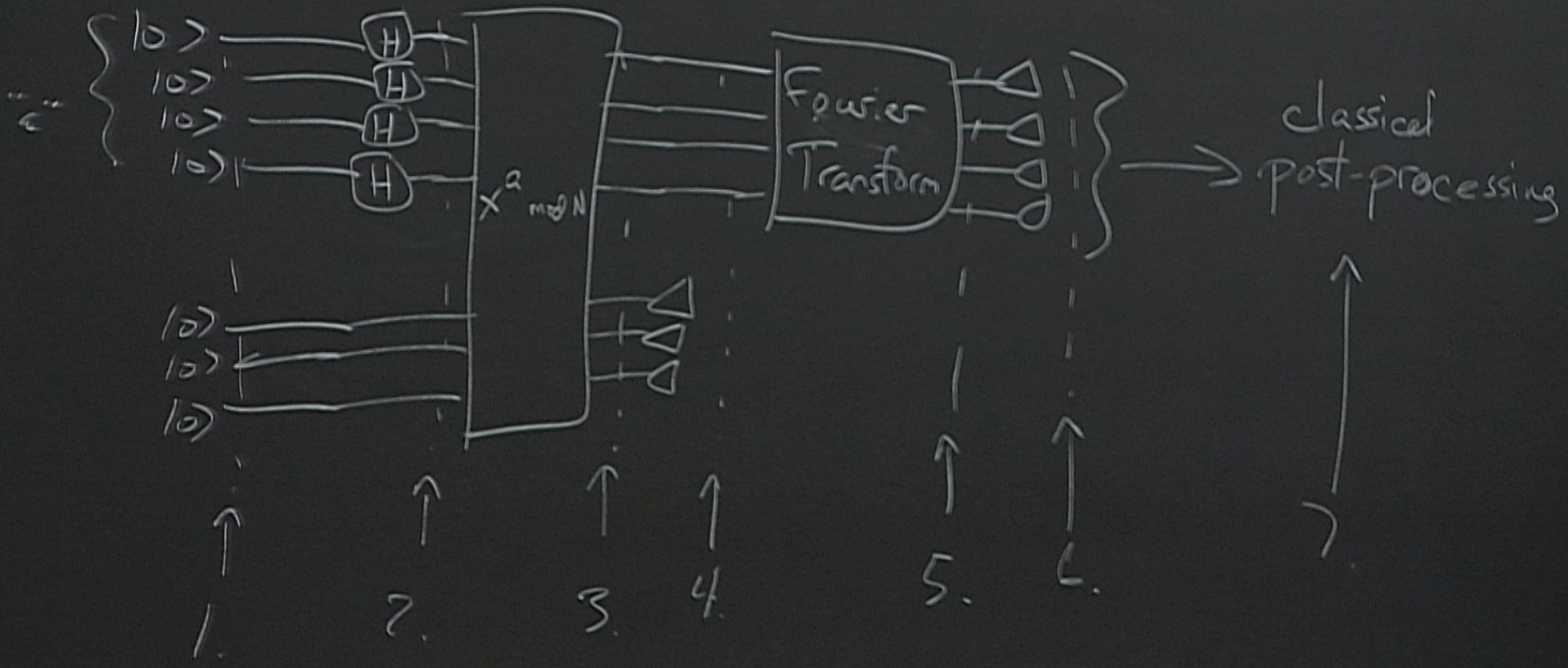
Fourier transform is mod 2^n FT.

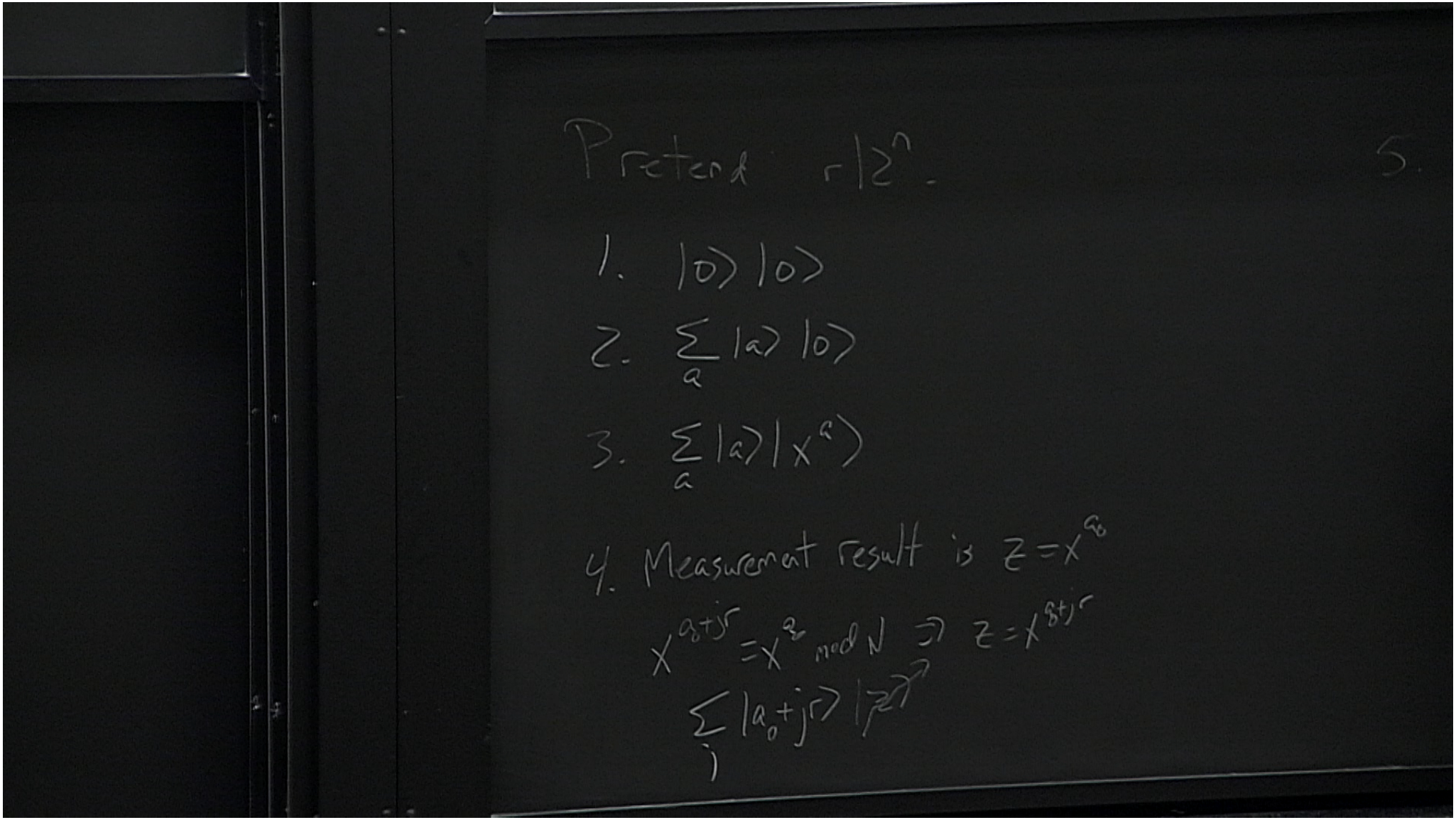
$$\mathcal{F}|a\rangle = \sum_b \omega^{ab} |b\rangle$$

$$\omega = e^{2\pi i / 2^n}$$

$x^q \bmod N$: $|a\rangle|c\rangle \mapsto |a\rangle|c + x^a \pmod N\rangle$

Shor's algorithm: x is given, find r s.t. $x^r = 1 \bmod N$.




Pretend $r|2^n$.
5.
1. $|0\rangle|0\rangle$
2. $\sum_a |a\rangle|0\rangle$
3. $\sum_a |a\rangle|x^a\rangle$
4. Measurement result is $z = x^{a_0}$
$x^{a_0+jr} = x^{a_0} \bmod N \Rightarrow z = x^{a_0+jr}$
$\sum_j |a_0+jr\rangle|z\rangle$

5. $\sum_j \sum_b \omega^{(a_0+jr)b} |b\rangle = \sum_b \omega^{a_0 b} \left[\sum_j e^{2\pi i jb/(2^n/r)}\right] |b\rangle$

$= \sum_c \omega^{a_0 c 2^n/r} |c2^n/r\rangle$

6. Measurement result is $c2^n/r$ for random c.

7. Repeat this a few times: $c_1 2^n/r$, $c_2 2^n/r$, $c_3 2^n/r$, ...

$GCD(c_1 2^n/r, c_2 2^n/r, \ldots) = 2^n/r$ with high probability $\Rightarrow$ Find r.

$$\sum_j e^{2\pi i j(b/\alpha)}$$

$$\alpha \mid b \Rightarrow \Sigma = \alpha$$

$$\alpha \nmid b \Rightarrow \Sigma = 0.$$