

# Lecture # 18, Quantum Computation 2: Quantum Protocols And Communications

Lecture notes of Isaac Chuang, transcribed by Jennifer Novosad

Administrata:

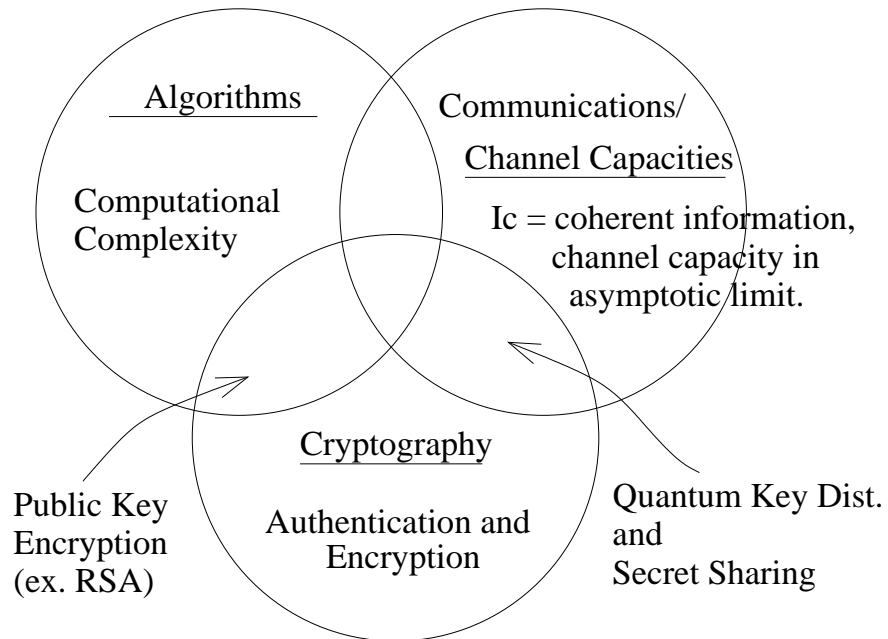
Projects will be presented in class in May, 3 presentations a day, 20 min slots. Sign up list is on the Wikki, first come first serve. Papers due May 12 (1/2 way between presentations).

Outline:

Tasks over a distributed set of parties

1. Perspective
2. Classical Communication Complexity
3. Ex. Fingerprinting (Q)
4. Digital Signatures
5. Q.D.S. Scheme

## 1. PERSPECTIVE



$I_c \simeq$  measure of trust

If a party shares a pure, entangled state, then it is only known to that party. So, it acts as a measure of trust.

How do you use it?

## 2. CLASSICAL COMMUNICATION COMPLEXITY

⇒ General setting

$f$  is publicly known

$$f : \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}$$

Alice:  $x \in \{0, 1\}^n$

Bob:  $y \in \{0, 1\}^n$

How much communication do they need to compute  $f$ ?

⇒ Options:

(1) Classical or Quantum bits

(2) Can compute answer with

- exactly (no error)
- bounded error  $\pm\epsilon$
- one sided error

...

(3) Assumptions

- Prior Shared Randomness (secret keys)
- Shared Entanglement

### 2.1. Example: Equality

$$f(x, y) = Eq(x, y) = \begin{cases} 0 & \text{if } x=y \\ 1 & \text{if otherwise} \end{cases}$$

$D(Eq) = n$  is deterministic or exact answer

$R(Eq) = ?$  is Random or Bounded error

2.1.1. *Randomized Protocol:*

⇒ Setup:

A and B agree on  $P > n/\epsilon$ , where  $\epsilon$  is the error and  $P$  is a prime.

Locally compute 2 polynomials over the field  $F(P)$ ,

$$A(z) = x_1 + x_2z + x_3z^2 + \dots + x_nz^{n-1}$$

$$B(z) = y_1 + y_2z + y_3z^2 + \dots + y_nz^{n-1}$$

Note for  $C(z) = A(z) - B(z)$ ,

$$x = y \rightarrow C(z) = 0$$

$$x \neq y \rightarrow (\# \text{ z's s.t. } C(z)=0) \leq n$$

⇒ Protocol:

A chooses random  $z \in F(P)$ . Sends  $(z, A(z))$

B computes  $C(z)$ , outputs EQ if  $C = 0$ , NEQ otherwise.

⇒ Analysis

$Prob(C(z) = 0, x \neq y) \leq n/p < \epsilon$ , by def. of  $P$  earlier.

A sends  $2 \log P$  bits =  $o(\log n - \log 1/\epsilon)$

$R(\text{EQ}) \sim O(\log n - \log 1/\epsilon) \cong O(\log n)$

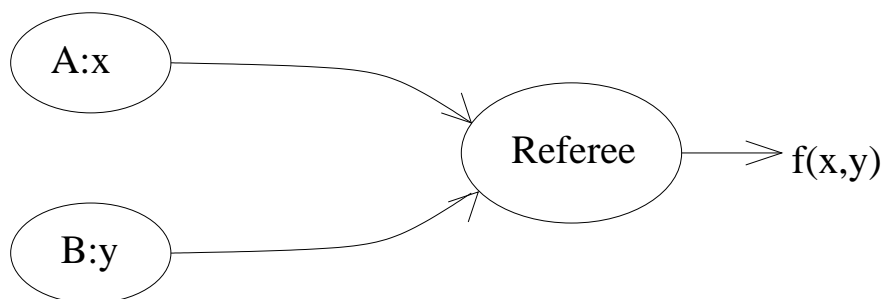
Approach: communicate the result of a function rather than the number itself.

## 2.2. Table of Costs

Problem	Exact Classical	R	Quantum Random	Quantum Exact
EQ	$n$	$\log n$	$\log n$	$n$
Parity/Inner Product	$n$	$n$	$n$	$n$
Dist J	$n$	$n$	$\sqrt{n}$	?
Distributed Deutsch Joza	$n$	$\log n$	$\log n$	$\log n$
RAZ (a promise function)		$n^{1/4}/\log n$	$\log n$	

### 3. FINGER PRINTING AS A SPECIFIC EXAMPLE

⇒ 3 party model, 1979, “simultaneous message passing” Andrew Yan



specific case where  $f(x, y) = EQ(x, y)$

⇒ Classical:  $\exists n \rightarrow m$  bit code with the following properties:

$$\{E(x) \in \{0, 1\}^m \mid x \in \{0, 1\}^n,$$

$$m = cn,$$

$$\text{dist}(E(x), E(y)) \geq (1 - \delta)m \text{ if } x \neq y\}$$

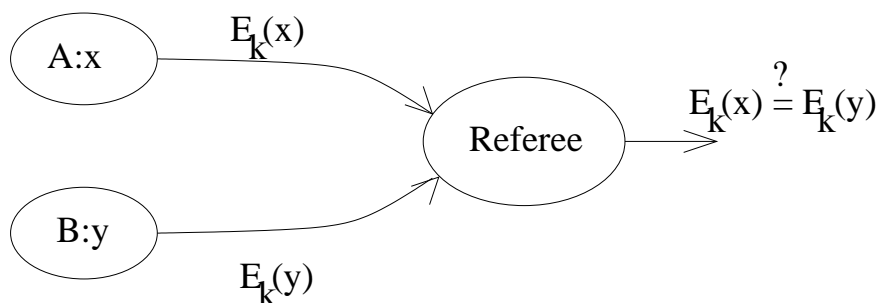
$\delta, c$  constants,  $E(x)$  code words,  $\text{dist} = \#$  different bits.

Example: Justen codes 1972

any  $c > 2$ ,  $\delta < \frac{9}{10} + \text{frac}115c$

Let  $E_i(x)$  denote the  $i^{\text{th}}$  bit of the code word. Suppose Alice and Bob share a secret key  $k \in \{0, 1\}^{\log m}$

#### 3.1. Protocol



Not Error:

$$Prob_{correct}(E_k(x) \neq E_k(y) | x \neq y) \geq 1 - \delta$$

Boosting: Repeat the protocol  $r$  times, with  $r$  values of  $k$ .  $Prob_{error} \rightarrow \delta^r$

Disadvantage: Need  $r$  secret keys

$\Rightarrow$  with no secret keys? Open problem from Yao, 1979

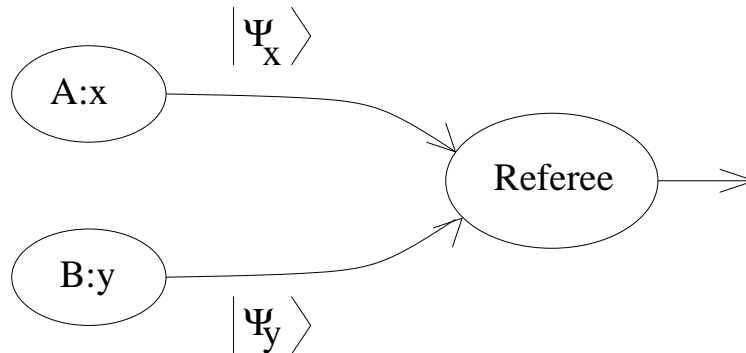
Solved in 1996, Ambians, Neuman to Szegedy, Babai

Requires  $\Omega(\sqrt{n})$  bits

$\Rightarrow$  Quantum Protocol for same problem

needs  $O(\log n)$  qubits without secret key

Buhrman, Cleve, Watrow 2001



where  $|\Psi_x\rangle$  and  $|\Psi_y\rangle$  are quantum bit strings.

### 3.2. Two Theorems

#### 3.2.1. Thm 1

$\exists 2^{2^m}$  states  $|\Psi_x\rangle$  of  $m$  qubits such that  $\langle \Psi_{x'} | \Psi_x \rangle \leq \delta$  for  $x' \neq x$  and  $\delta$  const (for some  $\delta$ ).  
(so, the states are not quite orthogonal.)

Proof:

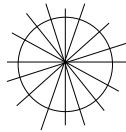
$$\text{Let } |\Psi_x\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |E_k(x)\rangle |k\rangle$$

Then:

$$\langle \Psi_x | \Psi_x \rangle = 1$$

$$\begin{aligned}
x \neq y &\rightarrow \langle \Psi_x | \Psi_y \rangle = \frac{1}{m} \sum_{kk'} \langle E_k(x) | E'_k(y) \rangle \langle k | k' \rangle \\
&= \frac{1}{m} \sum_k \langle E_k(x) | E_k(y) \rangle \\
&\leq m\delta/m = \delta \text{ bits the same, though } x \text{ and } y \text{ differ}
\end{aligned}$$

Note: stabilizers also work, or states on the unit circle



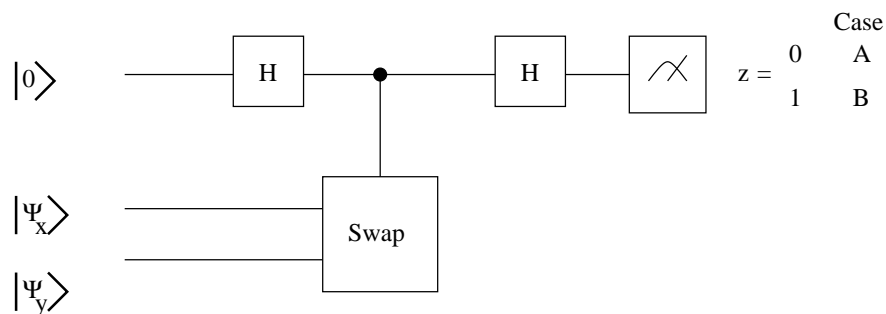
### 3.2.2. Thm 2

no-cloning  $\Rightarrow$  no perfect equality test.

Given 2 states  $|\Psi_x\rangle$  and  $|\Psi_y\rangle$  s.t. either  $|\Psi_x\rangle = |\Psi_y\rangle$  or  $|\Psi_x\rangle \neq |\Psi_y\rangle$  and  $|\langle \Psi_x | \Psi_y \rangle| \leq \delta$ ,  
Then which case is true can be determined with probability of error  $\leq \frac{1+\delta^2}{2}$

Proof:

Try to measure the operator swap



$$\begin{aligned}
|0, \Psi_x, \Psi_y\rangle &\rightarrow |0 + 1, \Psi_x, \Psi_y\rangle \\
&\rightarrow |0, \Psi_x, \Psi_y\rangle + |1, \Psi_x, \Psi_y\rangle \\
&\rightarrow |0 + 1, \Psi_x, \Psi_y\rangle + |0 - 1, \Psi_x, \Psi_y\rangle \\
&= |0\rangle(|\Psi_x, \Psi_y\rangle + |\Psi_y, \Psi_x\rangle) + |1\rangle(|\Psi_x, \Psi_y\rangle - |\Psi_y, \Psi_x\rangle)
\end{aligned}$$

First portion is symmetric case, second portion is antisymmetric case,  $= |\phi\rangle$

$$\begin{aligned}
\text{Prob}(z = 1 | x \neq y) &= \frac{1}{4} |\langle \phi | \phi \rangle|^2 \\
&= \frac{1}{4} |(\langle \Psi_x \Psi_y | - \langle \Psi_y \Psi_x |)(|\Psi_x \Psi_y\rangle - |\Psi_y \Psi_x\rangle)|
\end{aligned}$$

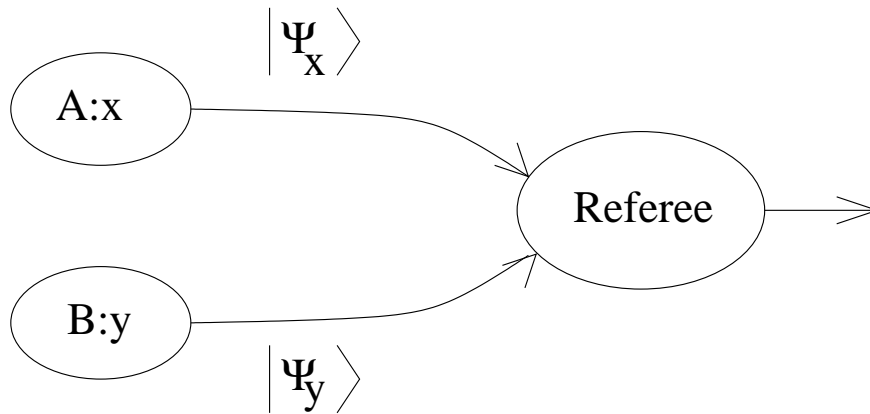
$$= \frac{1}{4}(2 - 2|\langle \Psi_x | \Psi_y \rangle|^2)$$

$$\leq \frac{1}{4}(2 - 2\delta^2) = \frac{1}{2}(1 - \delta^2)$$

Probability of Error  $\leq \frac{1}{2}(1 - \delta^2)$

Probabilistic equality test that requires a promise.

Finger Printing Protocol:



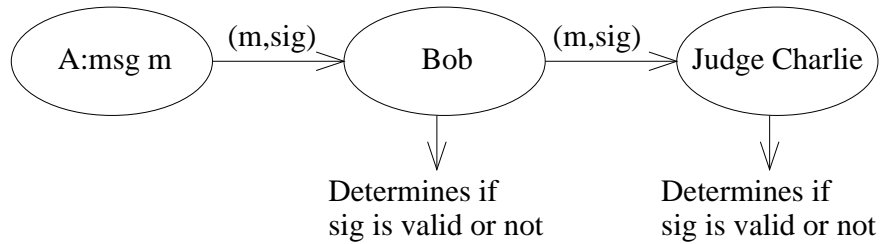
Probability of Error  $\leq \frac{1}{2}(1 - \delta^2) = \text{const.}$

Can boost this by repeating  $O(\log \frac{1}{\epsilon})$  times  $\rightarrow P_{error} < \epsilon$

Concept: Replaced shared randomness with qubits (this does not always work).

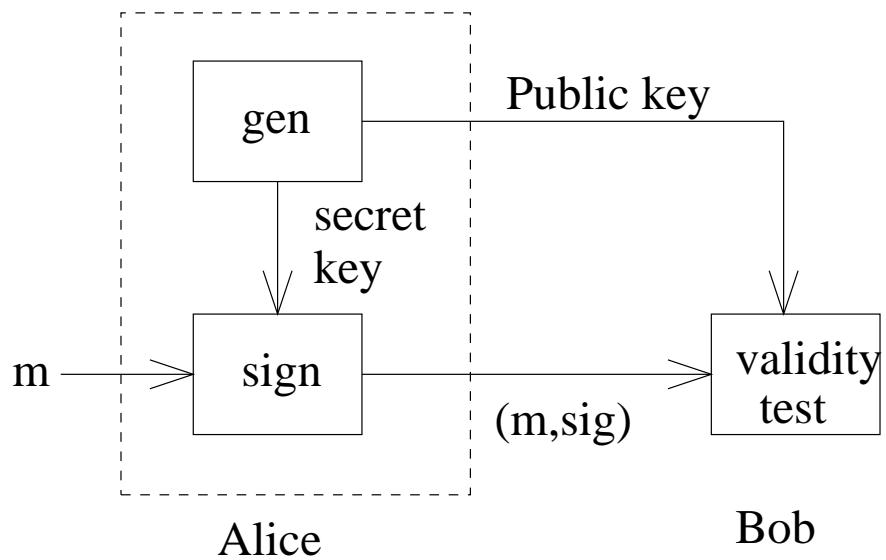
#### 4. DIGITAL SIGNATURE

Scenario:



Transferable msg Authentication

Classical Protocol



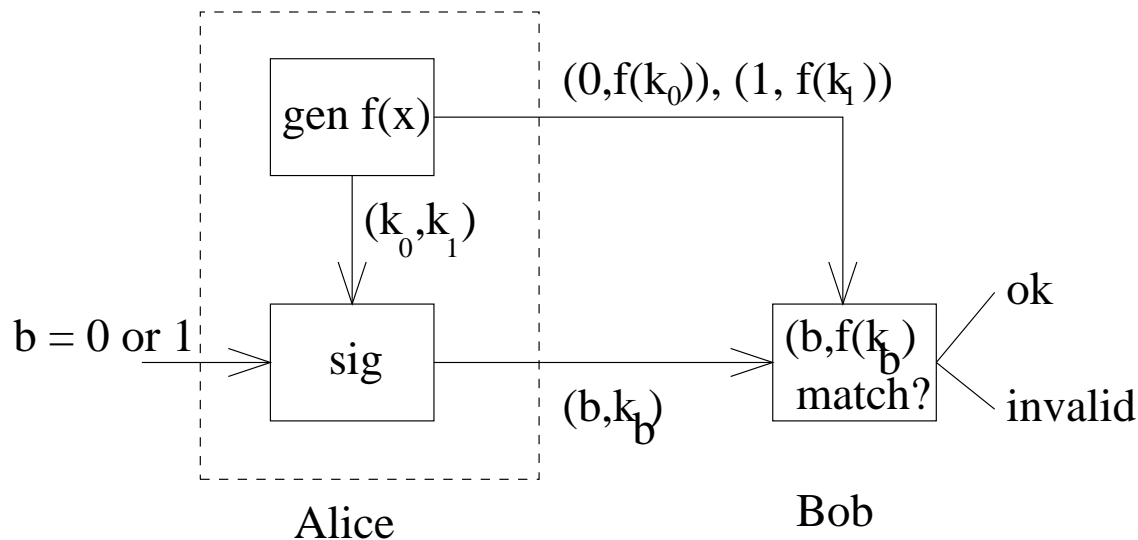
⇒ Desirable Properties

- (1) Not forgeable
- (2) Non-repudiatable
- (3) Efficient w.r.t. signature size (Keys reusable)

#### 4.1. One Time Classical Digital Signature Scheme (Lamport '79)

let  $f(x)$  be a one-way function (if you have  $x$ , getting  $f(x)$  is easy. If you have  $f(x)$ , you can't find  $x$ .  $f(x) \neq f(y)$ , or is exponentially rare.

$f(x)$  is public knowledge



example:

$$f([x, t]) = xy \quad k_0 = [7, 13], f(k_0) = 91 \quad k_1 = [3, 17], f(k_1) = 51$$

Public Key:  $(0, 91), (1, 51)$

msg's that you can send are  $[0, [7, 13]]$  or  $[1, [3, 17]]$ . Once sent, you've burned your key. It is not efficient.

Rompel: 1990: Info-secure DSS  $\Leftrightarrow$  One way function

Currently, we settle for computationally secure, but not informationally theoretic secure.

### 5. QUANTUM DIGITAL SECURITY SCHEME

Def:

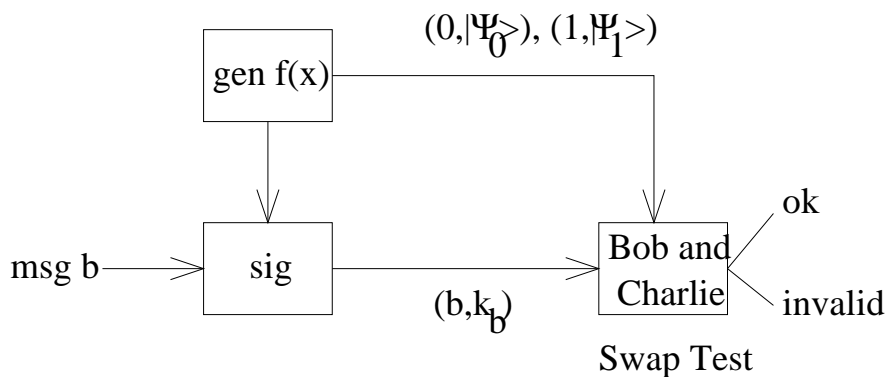
$$k \mapsto |\Psi_k\rangle$$

$k$  has  $l$  bits.  $|\Psi_k\rangle$  is the quantum fingerprint states from earlier, and has  $n$  qubits.  
 $n \sim O(\log l)$

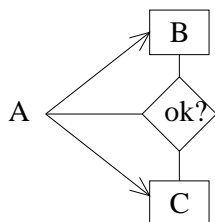
Claim:

This is a one way function, by Holevo's Thm. Can only extract  $n$  classical bits, given no prior entanglement.

Protocol:



Problem	Solution
Equality Test is probabilistic	$\Rightarrow$ Repeat: use $m$ keys for each $b$
$ \Psi_k\rangle$ leaks $\log l$ bits about $k$	$\Rightarrow$ Limit copies of public key to $T < \frac{l}{N}$ (so, only $T$ people can verify it)
Are all Public keys the same?	$\Rightarrow$ Symmetry test need certificate authority to check and distribute



⇒ Main Result

Info-theoretic one time public key secure D.S.S. whose classical msg  $b$  is signed by a classical private key string  $(\tilde{k}, b)$  corresponding to a public quantum key  $|\Psi_{\tilde{k}b}\rangle$

Resources Used

Size of  $b = 1$  bit

$\tilde{k}_b = O(LM)$  bits

$|\tilde{\Psi}_k\rangle = O(m \log L)$  qubits

# copies  $|\Psi_{\tilde{k}}\rangle \leq \frac{L}{\log L}$

Security

Prob[successful forgery]  $\leq e^{-(1-\frac{C_2}{1-\delta^2})M}$

Prob[successful repudiation]  $\leq e^{-|C_2-C_1|\sqrt{M}}$

where  $C_2$  and  $C_1$  are constants.

Problems

How to reuse keys?

How to reduce to using no Q.C. or Q. Memory

What are  $C_1$  and  $C_2$ ? (Existence proved by Gottesman and Chuang)

Physical Implementation