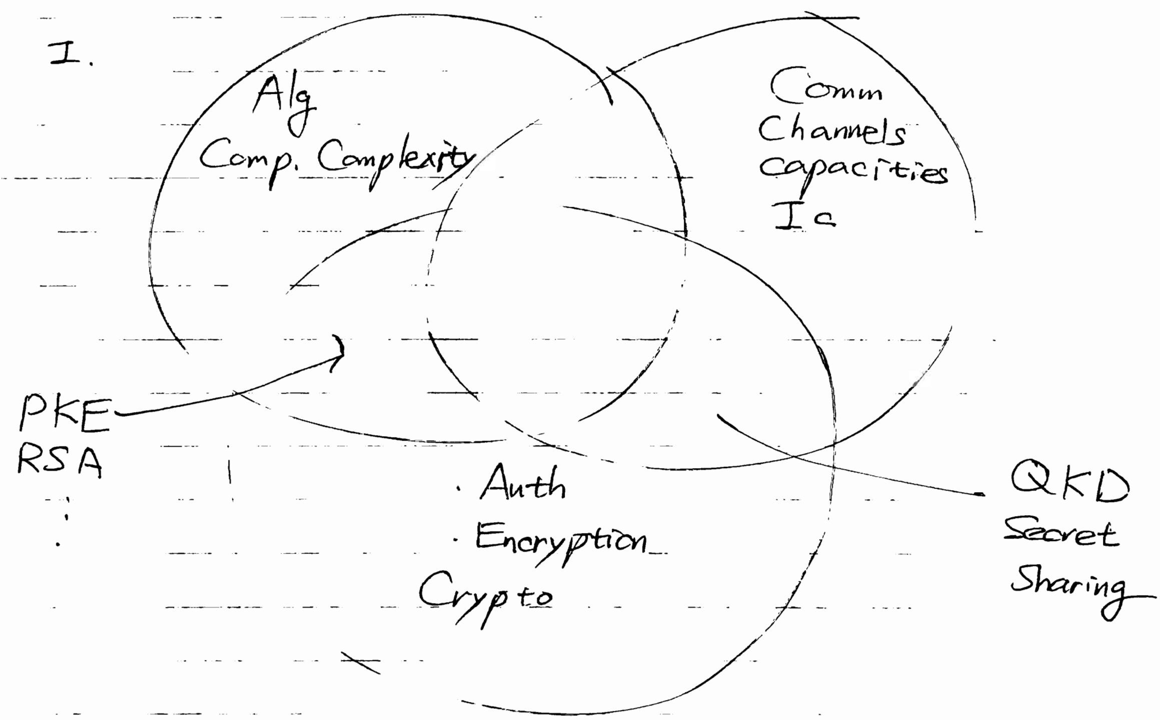
Lecture #18.
Q. Protocols & communications

I. Perspective
II. Classical comm. complexity
III. Ex. Fingerprinting (Q)
IV. Digital signatures
V. Q DSS

I.



$I_c \approx$ measure of trust

II. / Comm Cplxty

$\Rightarrow$ general setting

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

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

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

How much comm do they need to compute f?

$\Rightarrow$ Options : ① class / Q bits

② Compute – exactly (0-err)
– bounded error
– 1 sided error
⋮

③ shared randomness or entanglement

$\Rightarrow$ Ex : Equality $f(x,y) = EQ(x,y) = \begin{cases} 1 & x=y \\ 0 & \text{otherwise} \end{cases}$

Deterministic $D(EQ) = n$ exact

Random $R(EQ)$

Rand. Protocol

$\Rightarrow$ Setup : A & B agree on $P > n/\varepsilon$

Compute : $A(z) = x_1 + x_2 z + x_3 z^2 + \cdots + x_n z^{n-1}$

$B(z) = y_1 + y_2 z + y_3 z^2 + \cdots + y_n z^{n-1}$

↑ over $F(P)$

note for $C(z) = A(z) - B(z)$

$x = y \Leftrightarrow C = 0$

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

Protocol //

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

B computes $C(z)$ outputs EQ if $C=0$

NEQ other //

Analysis//

$$\text{Prob}(\underset{x \neq y}{C(z)=0}) \le \frac{n}{p} < \varepsilon$$

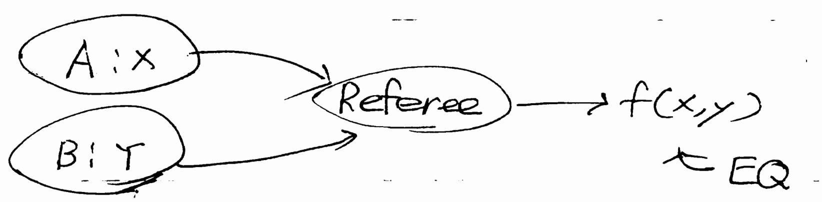
A sends $2 \log P = O(\log n + \log 1/\varepsilon)$,

$R(EQ) \sim O(\log n)$

Problem	Exact Cl	Random	Q	Q_E Quantum exact
EQ	n	$\log n$	$\log n$	n
Parity, inner product	n	n	n	n
DISJ	n	n	$\sqrt{n}$	?
Deutsch J.	n	$\log n$	$\log n$	$\log n$
RAZ		$n^{1/4}/\log n$	$\log n$	

III / Fingerprinting

$\Rightarrow$ 3 parity model "simlt. msg passing", Andrew Yao (1979)



$\Rightarrow$ Classical : $\exists\ n \to m$ code (classical)

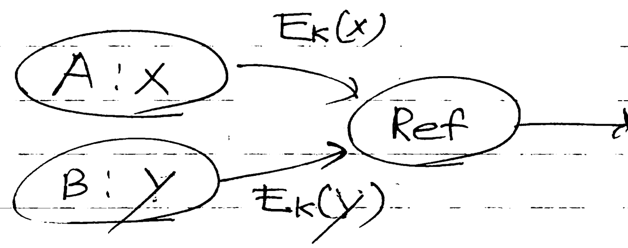
$$\left\{ \begin{array}{l} E(x) \in \{0,1\}^m \mid x \in \{0,1\}^n \\ \qquad m = Cn \\ \text{dist}(E(x), E(Y)) \ge (1-\delta)m, \quad \text{if } x \neq Y \\ \delta, c \text{ is constant} \end{array} \right\}$$

Ex. Justensen codes '72

any $c > 2$, $\delta < 9/10 + \frac{1}{15c}$

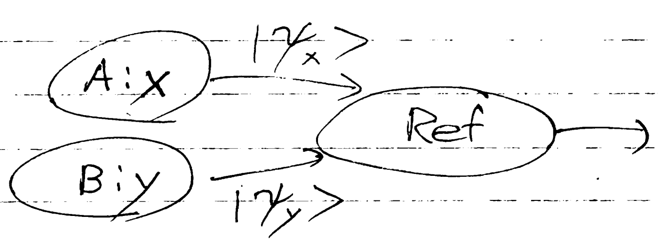
Let $E_i(x)$ denote i th bit.
Suppose A & B share a secret key $k \in \{0,1\}^{\log m}$

Protocol //



$\mathrm{Prob}(E_k(x) \neq E_k(y) \mid x \neq y) \geq 1-\delta$: correctness
δ is constant.
"Boosting" : repeat times
$\mathrm{Prob}(err) \rightarrow \delta^r$
Disadvantage : secret keys

$\Rightarrow$ With no secret key : open problem Yao '79
1996 : Ambainis , Babai
Newmann & Szegedy
$\Omega(\sqrt{n})$ bits
$\Rightarrow$ Q. Protocol
$\rightarrow$ needs $O(\log n)$ qubits, no secret key
Buhrman, Cleve, Watrow 2001



Two theorems

Thm ①: $\exists\ 2^{2^m}$ states $|\psi_x\rangle$ of m qubits satisfying $\langle\psi_{x'}|\psi_x\rangle \le \delta$, for $x \ne x'$ and δ const

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

Then $\langle\psi_x|\psi_x\rangle = 1$.

$$\langle\psi_x|\psi_y\rangle = \frac{1}{m}\sum_{k,k'}\langle k'|k\rangle\langle E_{k'}(x)|E_k(y)\rangle$$
$$= \frac{1}{m}\sum_k \langle E_k(x)|E_k(y)\rangle$$
$$\le \frac{1}{m}\cdot m\delta = \delta$$

note: stabilizers also work!

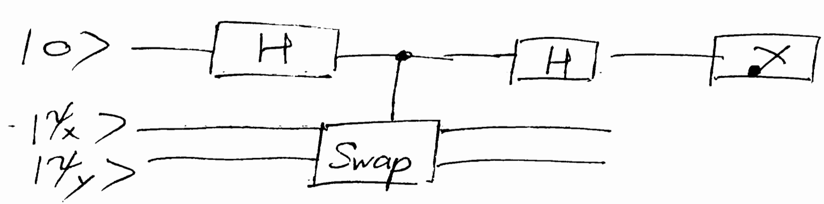
Thm ②: Given two state $|\psi_x\rangle, |\psi_y\rangle$ such that

A) $|\psi_x\rangle = |\psi_y\rangle$

or B) $|\langle\psi_x|\psi_y\rangle| \le \delta$

which one is true can be determined w. prob error $\le \frac{1+\delta^2}{2}$

Proof Swap test



$Z = \begin{matrix}0\\1\end{matrix}$ Case $\begin{matrix}A\\B\end{matrix}$

$$|0,\psi_x,\psi_y\rangle \to (0+1)(\psi_x\ \psi_y)$$
$$\to 0\psi_x\psi_y + 1\psi_y\psi_x$$
$$\to (0+1)\psi_x\psi_y + (0-1)\psi_y\psi_x$$
$$= 0(\underbrace{\psi_x\psi_y + \psi_y\psi_x}_{\text{symmetric}}) + 1(\underbrace{\psi_x\psi_y - \psi_y\psi_x}_{\text{anti symmetric}})$$
$$\equiv |\varphi\rangle$$

$$\mathrm{Prob}(z=1 \mid x\neq y) = |\langle\varphi|\varphi\rangle|^2 \cdot \frac{1}{4}$$
$$= \frac{1}{4}\left|\left(\langle\psi_x\psi_y| - \langle\psi_y\psi_x|\right)\left(|\psi_x\psi_y\rangle - |\psi_y\psi_x\rangle\right)\right|$$
$$= \frac{1}{4}\left(2 - 2|\langle\psi_x|\psi_y\rangle|^2\right)$$
$$\geq \frac{1}{2}(1-\delta^2)$$

Prob of err $\leq \frac{1}{2}(1+\delta^2)$

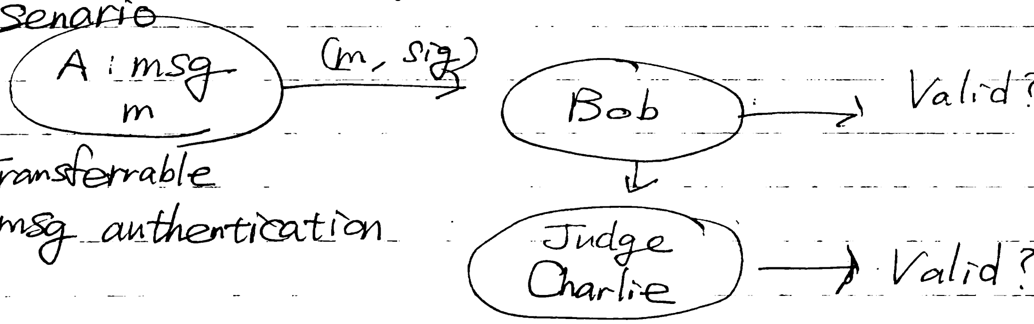
Note: No clonning theorem proves that there is no EQ (exact test).

Repeat: $O(\log\frac{1}{\varepsilon})$ times
$\longrightarrow P_{err} < \varepsilon$

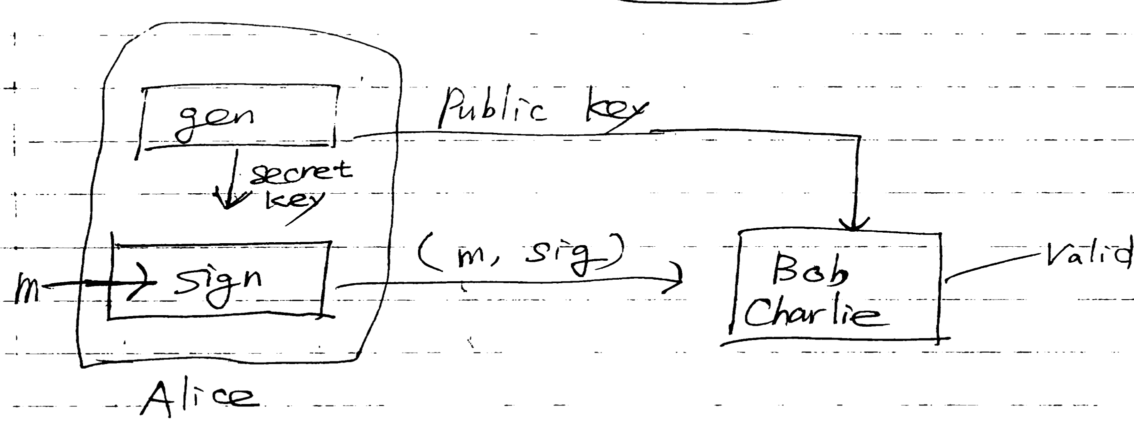
Concept: Replaced shared randomness with qubits!

IV / Digital signatures

Senario



Transferrable msg authentication



Desirable properties

① unforgeable

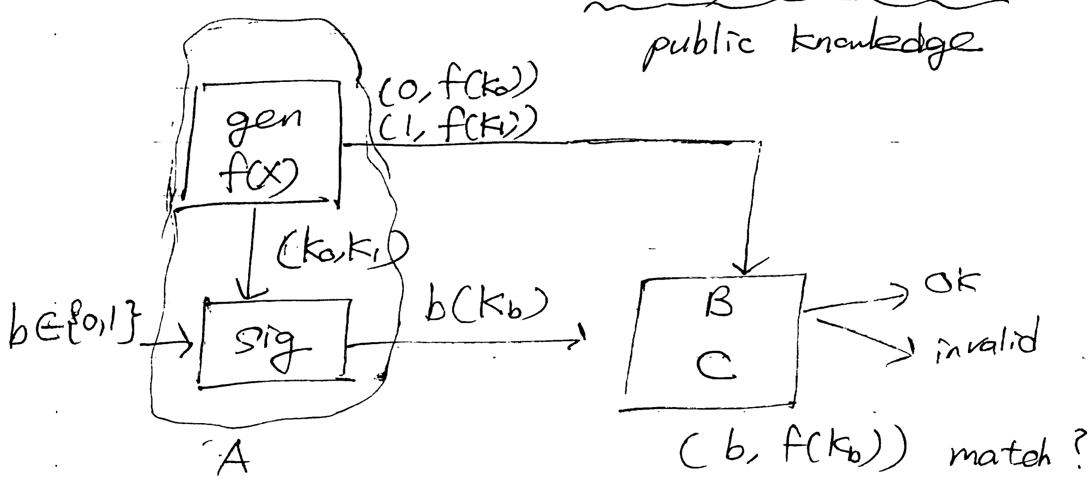
② Non-reputiable

③ efficient (keys reusable)

$\Rightarrow$ One-time classical DSS (Lamport '79)

Let $f(x)$ be a one-way function.

public knowledge



example

$f([x,y]) = xy$

$k_0 = [7, 13]$, $f(k_0) = 91$

$k_1 = [3, 17]$, $f(k_1) = 51$

Public keys $(0, 91)$, $(1, 51)$

msg $(0, [7, 13])$ msg $(1, [3, 17])$

Rompel '90 : Info-secure DSS

$\Leftrightarrow$ OWF one way function

V Quantum DSS

Def

$$\underbrace{K}_{L \text{ bits}} \longmapsto \underbrace{|f_K\rangle}_{n \text{ qubits}}$$

$n \sim O(\log L)$

Q. Fingerprinting states

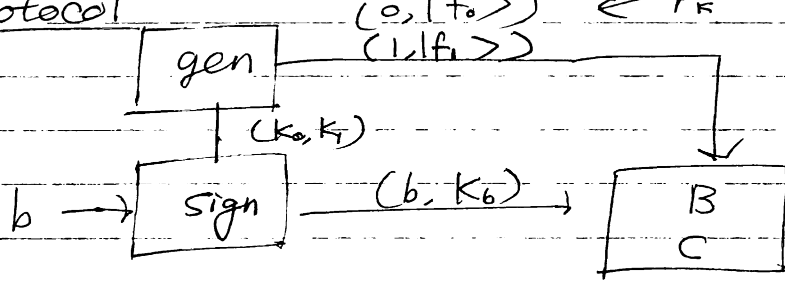
Claim

One-way function

pf

Holevo's theorem!

Protocol



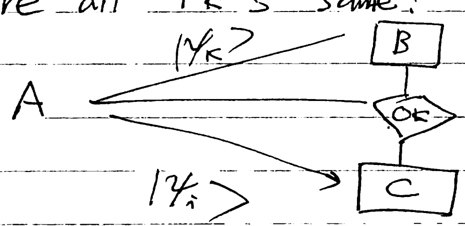
Swap test

Problem — Solution

EQ test is probabilistic $\Rightarrow$ Repeat: use m keys for each b

$|f_K\rangle$ leaks $\log l$ bits information about K $\Rightarrow$ limit copies to $T < L/n$

Are all P_K's same?



$\Rightarrow$ Symmetry test.

$\Rightarrow$ main result!

Info-theoretical secure one-time public key DSS whose classical msg b is signed by classical private key $(\tilde{k}_b)$ corresp. public quantum key $|f_{\tilde{k}_b}\rangle$.

Resource

size of(b) = 1 bit

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

$|f_k\rangle = O(m \log L)$ qubits

copies $|f_{\tilde{k}}\rangle \le \frac{L}{\log L}$

Security

Prob[Successful forgery] $\le e^{-(1-\frac{c_2}{1-\delta^2})m}$

Prob[Successful repu't.] $\le e^{-|c_2 - c_1|\sqrt{m}}$,

where c_1, c_2 const.

Problems to attack.

$\Rightarrow$ Ways to re-use keys?

$\Rightarrow$ Reduce to using no QC or Q memory.

$\Rightarrow$ what are c_1, c_2?

$\Rightarrow$ phys impl.