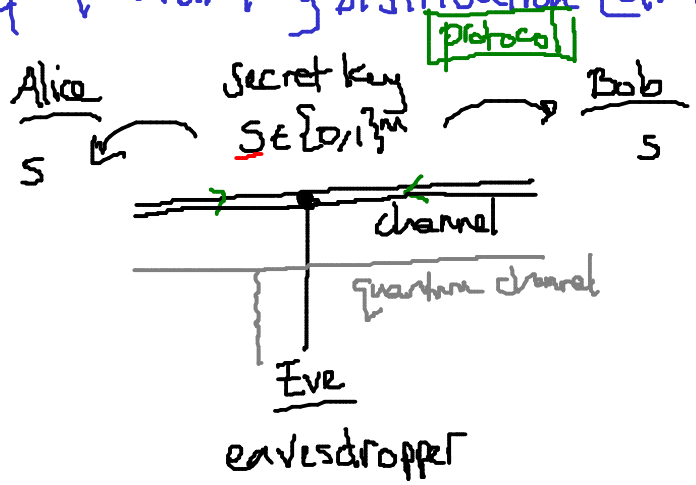
Measurements: p87 Mike & Ike

BB84 quantum Key Distribution (QKD) [Bennett, Brassard]



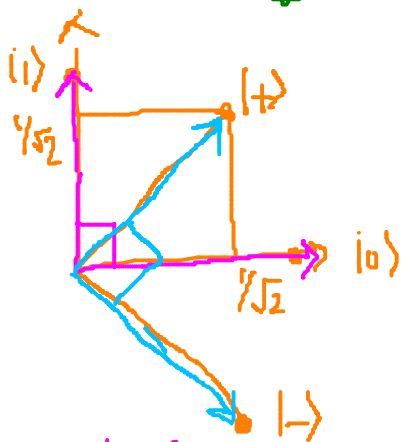
classical: assume hardness of certain number-theoretic problems
Diffie-Hellman (Discrete Logarithm)

quantum

Qubits: $\{|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}\}$ rectilinear basis R

$\{|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\}$ diagonal basis D

$\mathbb{C}^2$



$|0\rangle$ — H — $|+\rangle$

$|1\rangle$ — H — $|-\rangle$

Measurement: M_R M_D

$|\psi\rangle \to M_R \to \begin{cases}|0\rangle \text{ with prob } |a|^2\\ |1\rangle \text{ with prob } |b|^2\end{cases}$ $|a|^2+|b|^2=1$

$|\psi\rangle = a|0\rangle + b|1\rangle$

$|0\rangle \to M_D \to \begin{cases}|+\rangle\\ |-\rangle\end{cases}$

$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$

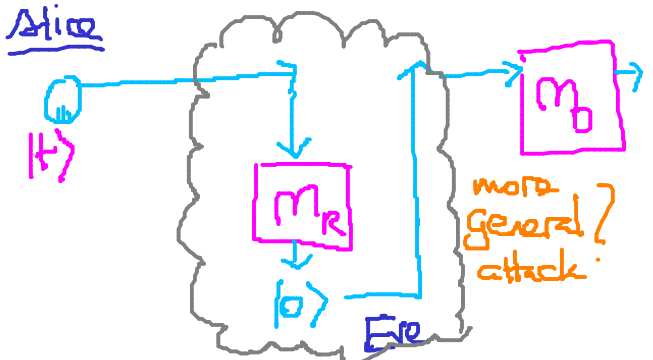
n qubits → $\sim \frac{n}{2}$ correct bases

BB84

Alice
- random basis

1 1 0
D R R D D R D R R R D
$|+\rangle|1\rangle|0\rangle|-\rangle|+\rangle|1\rangle|+\rangle|0\rangle|0\rangle|-\rangle$ classical
quantum channel
D D D R D R R R D R
$|+\rangle|+\rangle|-\rangle|0\rangle|+\rangle|1\rangle|0\rangle|0\rangle|-\rangle|1\rangle$
✓ × × × ✓ ✓ × ✓ × ×
1 1 1 0
Bob

How to detect Eve?



No Cloning Theorem

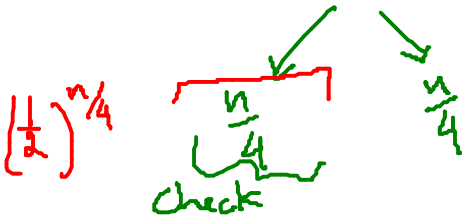
nonlinear

$|\psi_1\rangle|0\rangle \to |\psi_1\rangle|\psi_1\rangle$

$|\psi_2\rangle|0\rangle \to |\psi_2\rangle|\psi_2\rangle$ +

$\frac{1}{\sqrt{2}}\left(|\psi_1\rangle|0\rangle + |\psi_2\rangle|0\rangle\right) \to \frac{1}{\sqrt{2}}\left(|\psi_1\rangle|\psi_1\rangle + |\psi_2\rangle|\psi_2\rangle\right)$?? ✓

n qubits $\rightarrow \frac{n}{2}$ qubits



$\frac{|\psi_1\rangle + |\psi_2\rangle}{\sqrt{2}} |0\rangle \hookrightarrow (|\psi_1\rangle + |\psi_2\rangle)(|\psi_1\rangle + |\psi_2\rangle)$

Shor & Preskill (2000)

BB84 is secure (uses QECC)

Measurement operator

M observable:

Hermitian, positive semidefinite

$\Downarrow$

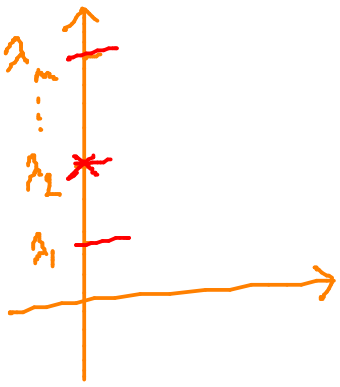
nonnegative eigenvalues

spectral decomposition

$$M = \sum_\lambda \lambda P_\lambda$$

P_λ: projector

energy levels



Measure a state $|\psi\rangle$ using operator M:

$\rightarrow p(\lambda) = \langle\psi| P_\lambda |\psi\rangle$ prob. of outcome λ

$\rightarrow$ State observed is $\frac{P_\lambda|\psi\rangle}{\sqrt{p(\lambda)}}$

$Tr(AB) = Tr(BA)$

$Tr(ABC) = Tr(CAB) = Tr(BCA)$

$Tr(P_\lambda \underbrace{|\psi\rangle\langle\psi|}_{\rho}) = Tr(\langle\psi| P_\lambda |\psi\rangle) = \langle\psi| P_\lambda |\psi\rangle$

ex: $R = \{P_0 = |0\rangle\langle 0|, P_1 = |1\rangle\langle 1|\}$

$P_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}; P_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \rightarrow p(0) = \langle\psi| P_0 |\psi\rangle$

$|\psi\rangle$ — R = $\begin{cases} |0\rangle & \text{with prob } |a|^2 \\ |1\rangle & \text{with prob } |b|^2 \end{cases}$

$= \begin{bmatrix} \bar{a} & \bar{b} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = |a|^2 = a\bar{a}$

$p(1) = |b|^2$ $\quad P_0|\psi\rangle = \begin{bmatrix} a \\ 0 \end{bmatrix}$

$$\frac{P_0|\psi\rangle}{\sqrt{p(0)}} = \frac{1}{|a|}\begin{bmatrix} a \\ 0 \end{bmatrix} = \frac{a}{|a|}|0\rangle = |0\rangle$$

Quantum state: $|\psi\rangle = \sum_b \alpha_b |b\rangle$ $\quad \alpha_b \in \mathbb{C}$ $\quad \sum_b |\alpha_b|^2 = 1$

$\equiv$ $b \in \{0,1\}^n$ $\quad b = b_1 b_2 \dots b_n$ $\quad b_i \in \{0,1\}$

pure state

↓ [von Neumann]

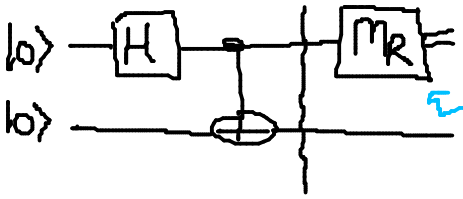
$|b\rangle = \underbrace{|b_1\rangle}_{\mathbb{C}^2} \underbrace{|b_2\rangle}_{\mathbb{C}^2} \dots \underbrace{|b_n\rangle}_{\mathbb{C}^2} \in \mathbb{C}^{2^n}$

mixed state

density matrix $\rho = \underbrace{\sum_i p_i |\psi_i\rangle\langle\psi_i|}_{\text{distribution over pure states}}$ $\quad \sum_i p_i = 1$ $\quad 0 \le p_i \le 1$

Bell circuit

$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)$



$\langle\psi| = \frac{1}{\sqrt{2}}(\langle 0|\otimes\langle 0| + \langle 1|\otimes\langle 1|)$

partial measurement

$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$(A\otimes B)^\dagger = A^\dagger \otimes B^\dagger$

$(A\otimes B)(C\otimes D) = AC \otimes BD$

$\rho = |\psi\rangle\langle\psi| = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)$

rank 1 matrix

$= \frac{1}{2}(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)\cdot(\langle 0|\otimes\langle 0| + \langle 1|\otimes\langle 1|)$

$= \frac{1}{2}\left((|0\rangle\otimes|0\rangle)(\langle 0|\otimes\langle 0|) + (|0\rangle\otimes|0\rangle)(\langle 1|\otimes\langle 1|) + \dots\right)$

$= \frac{1}{2}\Big(\underbrace{|0\rangle\langle 0|}_{\text{trace}}\otimes|0\rangle\langle 0| + \underbrace{|0\rangle\langle 1|}_{\text{trace}}\otimes|0\rangle\langle 1| + |1\rangle\langle 0|\otimes|1\rangle\langle 0| + \underbrace{|1\rangle\langle 1|}_{\text{trace}}\otimes|1\rangle\langle 1|\Big)$

$= \frac{1}{2}\Big(\underbrace{\langle 0|0\rangle}_{=1}\otimes|0\rangle\langle 0| + \underbrace{\langle 1|0\rangle}_{=0}\otimes|0\rangle\langle 1| + \underbrace{\langle 0|1\rangle}_{=0}\otimes|1\rangle\langle 0| + \underbrace{\langle 1|1\rangle}_{1}\otimes|1\rangle\langle 1|\Big)$

$\tilde{\rho} = \underbrace{\frac{1}{2}|0\rangle\langle 0|}_{\rho_0} + \underbrace{\frac{1}{2}|1\rangle\langle 1|}_{\rho_1} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$

Hamiltonian Simulation

QLS: Quantum Linear System [Harrow, Hassidim, Lloyd]

given matrix A and vector $\underline{b}$, compute x s.t. $Ax = b$

$x = A^{-1}b$

Hermitian ✓ invertible ✓

$A = \sum_i \lambda_i |z_i\rangle\langle z_i|$ spectral theorem

Hamiltonian Simulation: unitary e^{iAt} ??

$A^{-1} = \sum_i \frac{1}{\lambda_i} |z_i\rangle\langle z_i| \Rightarrow A^{-1}|b\rangle = \sum_i \frac{1}{\lambda_i} |z_i\rangle\langle z_i|b\rangle$ (scalar)

$= \sum_i \frac{1}{\lambda_i} \langle z_i|b\rangle |z_i\rangle$

$|b\rangle \longrightarrow \sum_j \langle z_j|b\rangle e^{i\lambda_j t} |z_j\rangle|0\rangle$

phase estimation $\longrightarrow \sum_j \langle z_j|b\rangle e^{i\lambda_j t} |z_j\rangle|\lambda_j t\rangle|0\rangle$

$e^{iAt}|b\rangle = I|b\rangle = \sum_i |z_i\rangle\langle z_i| \; \sum_i \langle z_i|b\rangle |z_i\rangle$

$\longrightarrow \sum_j \langle z_j|b\rangle e^{i\lambda_j t} \frac{C}{\lambda_j t} |z_j\rangle|\lambda_j t\rangle|0\rangle$ $= \sum_i \langle z_i|b\rangle e^{i\lambda_i t}|z_i\rangle$

un-Phase estimation $\longrightarrow \sum_j \langle z_j|b\rangle e^{i\lambda_j t} \frac{C}{\lambda_j t} |z_j\rangle|0\rangle|0\rangle \longrightarrow \left(\frac{C}{\lambda_j t}\right)|b\rangle + \sqrt{1 - \frac{C^2}{(\lambda_j t)^2}}|1\rangle$

undo e^{iAt} $\longrightarrow \left[\sum_j \langle z_j|b\rangle \frac{C}{\lambda_j t} |z_j\rangle|0\rangle|0\rangle\right] = |x\rangle$

Hamiltonian Simulation:
Given A, implement/run $e^{iAt} = I + itA - \frac{t^2A^2}{2} + \cdots$

truncated Taylor?

Trotter-Suzuki H

$e^{i(A+B)} \cong e^{iA} e^{iB} e^{i[A,B]}$ + error

Sequential

$e^{i(A+B)}|\psi\rangle = e^{iA} e^{iB} |\psi\rangle$

$A \Rightarrow e^{iAt} \Rightarrow \lambda_i \Rightarrow \frac{1}{\lambda_i}$

N. Wiebe's talk?

Latest work on QLS: A^{-1} ($\frac{1}{A}$) using Taylor approx of $\left(\frac{1}{x}\right)$ — quantum walk?

Gottesman-Chuang